

---

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

---

In Re U.S. Patent Application )

Applicant: Kawasaki et al. )


Serial No. )

Filed: September 15, 2003 )

For: LICENSE ISSUANCE SERVER, )  
PROCESSING DEVICE, )  
SOFTWARE EXECUTION )  
MANAGEMENT DEVICE, AND )  
LICENSE ISSUING METHOD )  
AND PROGRAM )

*I hereby certify that this paper is being deposited with the United States Postal Service as EXPRESS MAIL in an envelope addressed to: Mail Stop PATENT APPLICATION, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this date.*

9-15-03  
Date

  
Express Mail Label No.: EV032734935US

**CLAIM FOR PRIORITY**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

Applicants claim foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

Japanese Patent Application No. 2002-274845, filed September 20, 2002

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS &amp; CRAIN, LTD.

By



Patrick G. Burns  
Registration No. 29,367

September 15, 2003  
300 South Wacker Drive  
Suite 2500  
Chicago, Illinois 60606  
Telephone: 312.360.0080  
Facsimile: 312.360.9315

1/8

0828.68359  
(312) 360.0080

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 2 年   9 月 2 0 日  
Date of Application:

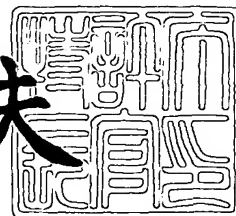
出 願 番 号            特 願 2 0 0 2 - 2 7 4 8 4 5  
Application Number:  
[ST. 10/C] :            [ J P 2 0 0 2 - 2 7 4 8 4 5 ]

出      願      人            富 士 通 株 式 会 社  
Applicant(s):

2 0 0 3 年   7 月 2 4 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号   出証特 2 0 0 3 - 3 0 5 8 8 8 5

---

【書類名】 特許願

【整理番号】 0252364

【提出日】 平成14年 9月20日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 9/06 550

【発明の名称】 ライセンス発行サーバ、処理装置、ソフトウェア実行管理装置、ライセンス発行方法、ライセンス発行プログラム

【請求項の数】 10

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 川崎 高司

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 笹森 幸一

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 品川 雅之

【特許出願人】

    【識別番号】 000005223

    【氏名又は名称】 富士通株式会社

【代理人】

    【識別番号】 100092152

    【弁理士】

    【氏名又は名称】 服部 毅巖

    【電話番号】 0426-45-6644

---

**【手数料の表示】****【予納台帳番号】** 009874**【納付金額】** 21,000円**【提出物件の目録】****【物件名】** 明細書 1**【物件名】** 図面 1**【物件名】** 要約書 1**【包括委任状番号】** 9705176**【プルーフの要否】** 要

【書類名】 明細書

【発明の名称】 ライセンス発行サーバ、処理装置、ソフトウェア実行管理装置、ライセンス発行方法、ライセンス発行プログラム

【特許請求の範囲】

【請求項 1】 ソフトウェアの実行ライセンスを発行するライセンス発行サーバにおいて、

前記ソフトウェアの暗号化のための暗号キー生成要求に応じて、ソフトウェア暗号キーと、前記ソフトウェア暗号キーで暗号化された前記ソフトウェアを復号するためのソフトウェア復号キーとを生成するソフトウェア暗号キー生成手段と、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含むライセンス発行要求に応じて、前記装置識別情報を暗号キーとして前記ソフトウェア復号キーを暗号化し、暗号化された前記ソフトウェア復号キーを含むソフトウェアライセンスを出力するライセンス発行手段と、  
を有することを特徴とするライセンス発行サーバ。

【請求項 2】 ライセンスによって実行が制限されたソフトウェアを実行する処理装置において、

装置識別情報が固定的に記録された記録媒体と、

暗号化された状態のソフトウェア復号キーを受け取ると、前記記録媒体に記録された前記装置識別情報を復号キーとして前記ソフトウェア復号キーを復号する復号キー復号手段と、

暗号化された状態の前記ソフトウェアを受け取ると、前記復号キー復号手段で復号された前記ソフトウェア復号キーを復号キーとして前記ソフトウェアを復号するソフトウェア復号手段と、

を有することを特徴とする処理装置。

【請求項 3】 ソフトウェアの実行ライセンスを発行するライセンス発行サーバにおいて、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含む着脱キー情報生成要求に应答して、前記装置識別情報

と着脱キー固有暗号キーとを含む着脱キー情報を生成し、生成した前記着脱キー情報を、前記処理装置に着脱可能なハードウェアキーに記録する着脱キー情報発行手段と、

前記ソフトウェアのライセンス発行要求に応じて、暗号化された状態で提供される前記ソフトウェアを復号するためのソフトウェア復号キーを前記着脱キー固有暗号キーで暗号化して、暗号化された前記ソフトウェア復号キーを含むライセンス情報を出力するライセンス発行手段と、

を有することを特徴とするライセンス発行サーバ。

【請求項 4】 前記ライセンス発行手段により出力された前記ライセンス情報の履歴を蓄積し、蓄積された前記ライセンス情報に基づいて、前記ソフトウェアの提供者に対して請求するライセンス発行手数料を算出するライセンス発行費用算出手段をさらに有することを特徴とする請求項 3 記載のライセンス発行サーバ。

【請求項 5】 ライセンスによって実行が制限されたソフトウェアを実行する処理装置において、

装置識別情報が固定的に記録された記録媒体と、

動作許可対象装置を特定する許可対象装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報が格納されたハードウェアキーが装着されたとき、前記ハードウェアキーから前記着脱キー情報を読み取るハードウェアキー接続手段と、

暗号化された状態の前記ソフトウェアを提供するソフトウェア提供サーバから、前記ソフトウェアを復号するためのソフトウェア復号キーが暗号化された状態で含まれたライセンス情報を取得するライセンス取得手段と、

前記ソフトウェア復号キーを前記着脱キー固有暗号キーで復号するソフトウェアキー復号手段と、

前記ハードウェアキー接続手段に接続された前記ハードウェアキーに含まれる前記許可対象識別情報と前記記録媒体に記録された装置識別情報との同一性を判定する識別情報判定手段と、

前記識別情報判定手段により、同一であると判定された場合には、前記ソフトウェアキー復号手段で復号された前記ソフトウェア復号キーで、暗号化された状

態の前記ソフトウェアを復号するソフトウェア復号手段と、  
を有することを特徴とする処理装置。

【請求項 6】 ライセンスによって実行が制限されたソフトウェアの実行状況を管理するソフトウェア実行管理装置において、

装置識別情報が固定的に記録された記録媒体と、

動作許可対象装置を特定する許可対象装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報が格納されたハードウェアキーが装着されたとき、前記ハードウェアキーから前記着脱キー情報を読み取るハードウェアキー接続手段と、

暗号化された状態の前記ソフトウェアを復号するための暗号化されたソフトウェア復号キーと同時実行可能なコンピュータ数とが含まれたライセンス情報が入力されると、前記ソフトウェア復号キーを前記着脱キー固有暗号キーで復号するソフトウェアキー復号手段と、

ネットワークを介して接続されたコンピュータのうち前記ソフトウェアを実行している実行コンピュータ数を監視し、前記同時実行可能なコンピュータ数以下の数の前記コンピュータに対して、前記ソフトウェアキー復号手段で復号された前記ソフトウェア復号キーを渡す復号キー管理手段と、

を有することを特徴とするソフトウェア実行管理装置。

【請求項 7】 ソフトウェアの実行ライセンスを発行するためのライセンス発行方法において、

前記ソフトウェアの暗号化のための暗号キー生成要求に応じて、ソフトウェア暗号キーと、前記ソフトウェア暗号キーで暗号化された前記ソフトウェアを復号するためのソフトウェア復号キーとを生成し、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含むライセンス発行要求に応じて、前記装置識別情報を暗号キーとして前記ソフトウェア復号キーを暗号化し、暗号化された前記ソフトウェア復号キーを含むソフトウェアライセンスを出力する、

ことを特徴とするライセンス発行方法。

【請求項 8】 ソフトウェアの実行ライセンスを発行するためのライセンス発行方法において、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含む着脱キー情報生成要求に応答して、前記装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報を生成し、生成した前記着脱キー情報を、前記処理装置に着脱可能なハードウェアキーに記録し、

前記ソフトウェアのライセンス発行要求に応じて、暗号化された状態で提供される前記ソフトウェアを復号するためのソフトウェア復号キーを前記着脱キー固有暗号キーで暗号化して、暗号化された前記ソフトウェア復号キーを含むライセンス情報を出力する、

ことを特徴とするライセンス発行方法。

【請求項 9】 ソフトウェアの実行ライセンスを発行するためのライセンス発行プログラムにおいて、

コンピュータに、

前記ソフトウェアの暗号化のための暗号キー生成要求に応じて、ソフトウェア暗号キーと、前記ソフトウェア暗号キーで暗号化された前記ソフトウェアを復号するためのソフトウェア復号キーとを生成し、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含むライセンス発行要求に応じて、前記装置識別情報を暗号キーとして前記ソフトウェア復号キーを暗号化し、暗号化された前記ソフトウェア復号キーを含むソフトウェアライセンスを出力する、

処理を実行させることを特徴とするライセンス発行プログラム。

【請求項 10】 ソフトウェアの実行ライセンスを発行するためのライセンス発行プログラムにおいて、

コンピュータに、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含む着脱キー情報生成要求に応答して、前記装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報を生成し、生成した前記着脱キー情報を、前記処理装置に着脱可能なハードウェアキーに記録し、

前記ソフトウェアのライセンス発行要求に応じて、暗号化された状態で提供される前記ソフトウェアを復号するためのソフトウェア復号キーを前記着脱キー固

有暗号キーで暗号化して、暗号化された前記ソフトウェア復号キーを含むライセンス情報を出力する、

処理を実行させることを特徴とするライセンス発行プログラム。

#### 【発明の詳細な説明】

#### 【0001】

##### 【発明の属する技術分野】

本発明はソフトウェアの実行内容をライセンスで制限するためのライセンス発行サーバ、処理装置、ソフトウェア実行管理装置、ライセンス発行方法、ライセンス発行プログラムに関し、特に不正なライセンス取得を防止したライセンス発行サーバ、処理装置、ソフトウェア実行管理装置、ライセンス発行方法、ライセンス発行プログラムに関する。

#### 【0002】

##### 【従来の技術】

一般にソフトウェアを販売するとき、購入者に対して、そのソフトウェアを使用するためのライセンスを与える。ライセンスの内容としては、コンピュータの同時使用台数の制限、使用期間の制限、マルチユーザシステムにおける同時使用ユーザ数の制限などである。

#### 【0003】

ところが、近年、ライセンスの内容を超えたソフトウェアの不正使用が社会問題となっている。たとえば、市販されている多くのソフトウェアでは、ソフトウェアのライセンス条項において1つのコンピュータでの使用しか認めていない。ところが、そのソフトウェアが不正使用防止機能を備えていないと、そのソフトウェアを多数のコンピュータで使用することが容易にできてしまう。

#### 【0004】

そこで、ソフトウェアの不正使用を防止するための様々な技術が開発されている。ソフトウェアの不正使用の防止技術として、コンピュータ固有の識別情報を用いたものがある。

#### 【0005】

たとえば、ライセンスコードおよびマシン識別コードから生成したマシン固有

のソフトウェア使用コードによりソフトウェア使用チェックを行うソフトウェア管理方法がある（例えば、特許文献1参照）。なお、特許文献1では、マシン識別コードとして、ソフトウェアが稼働するコンピュータマシンのOS（Operating System）名、OS番号、ソフトウェアが導入されたハードディスク番号を含むことが示されている（特許文献1、段落[0031]）。

#### 【0006】

##### 【特許文献1】

特開2000-207199号公報

#### 【0007】

##### 【発明が解決しようとする課題】

しかし、特許文献1に記載された発明では、マシン識別コードとして、OS名やOS番号が使用されていると、ライセンス供与を受けたマシンのOSが不正にコピーされた場合、コピーされたOS上でもソフトウェアが起動できてしまう。さらに、ハードディスク番号は、コンピュータ毎にOSによって定義される番号である。そのため、マシン識別コードにハードディスク番号が含まれていても、不正コピーしたソフトウェアを元と同じハードディスク番号のハードディスクに導入すれば、そのソフトウェアを起動できてしまう。

#### 【0008】

このように、特許文献1のソフトウェア管理方法では、マシン識別コードに含まれる情報の複写が容易であることにより、ライセンスでの制限を超えたソフトウェアの不正使用が容易であった。

#### 【0009】

本発明はこのような点に鑑みてなされたものであり、マシン毎のライセンス供与に関する強固な不正防止機能を実現したライセンス発行サーバ、処理装置、ソフトウェア実行管理装置、ライセンス発行方法、ライセンス発行プログラムを提供することを目的とする。

#### 【0010】

##### 【課題を解決するための手段】

本発明の第1の態様では上記課題を解決するために、図1に示すようなライセ

ンス発行サーバが提供される。第1の態様に係るライセンス発行サーバは、ソフトウェアの実行ライセンスを発行するものであり、以下の機能を有している。

【0011】

ソフトウェア暗号キー生成手段1は、ソフトウェア6aの暗号化のための暗号キー生成要求に応じて、ソフトウェア暗号キー5aと、ソフトウェア暗号キー5aで暗号化されたソフトウェア6bを復号するためのソフトウェア復号キー5bとを生成する。ライセンス発行手段2は、ソフトウェア6aの動作許可対象である処理装置4内の記録媒体4aに固定的に記録された装置識別情報4bを含むライセンス発行要求に応じて、装置識別情報4bでソフトウェア復号キー5bを暗号化し、暗号化されたソフトウェア復号キーを含むソフトウェアライセンス5cを出力する。

【0012】

このようなライセンス発行サーバによれば、ソフトウェア復号キー5bを装置識別情報4bで暗号化しているため、その装置識別情報4bが固定的に記録された処理装置4でのみ暗号化されたソフトウェアを復号することが可能となる。

【0013】

本発明の第2の態様では上記課題を解決するために、ライセンスによって実行が制限されたソフトウェアを実行する処理装置において、装置識別情報が固定的に記録された記録媒体と、暗号化された状態のソフトウェア復号キーを受け取ると、前記記録媒体に記録された前記装置識別情報を復号キーとして前記ソフトウェア復号キーを復号する復号キー復号手段と、前記ソフトウェア提供サーバから暗号化された状態の前記ソフトウェアを受け取ると、前記復号キー復号手段で復号された前記ソフトウェア復号キーを復号キーとして前記ソフトウェアを復号するソフトウェア復号手段と、を有することを特徴とする処理装置が提供される。

【0014】

このような処理装置によれば、記録媒体に固定的に記録された装置識別情報で暗号化されたソフトウェア復号キーを取得した場合に限り、そのソフトウェア復号キーを復号することができる。

【0015】

本発明の第3の態様では上記課題を解決するために、図7に示すようなライセンス発行サーバが提供される。第3の態様に係るライセンス発行サーバは、ソフトウェアの実行ライセンスを発行するものであり、以下の機能を有している。

【0016】

着脱キー情報発行手段91は、ソフトウェア99aの動作許可対象である処理装置94内の記録媒体94aに固定的に記録された装置識別情報91bを含む着脱キー情報生成要求に応答して、装置識別情報91bと着脱キー固有暗号キー91cとを含む着脱キー情報91aを生成し、生成した着脱キー情報91aを、処理装置94に着脱可能なハードウェアキー96に記録する。ライセンス発行手段92は、ソフトウェアのライセンス発行要求に応じて、暗号化された状態で提供されるソフトウェア99aを復号するためのソフトウェア復号キー98aを着脱キー固有暗号キー91cで暗号化して、暗号化されたソフトウェア復号キー98cを含むライセンス情報98bを出力する。

【0017】

このようなライセンス発行サーバによれば、正しいハードウェアキー96が装着された処理装置94に限りライセンス情報を復号し、暗号化された状態のソフトウェア99bを復号することができる。しかも、装置識別情報がハードウェアキー96に格納されていることにより、装置識別情報が合致する処理装置でのみソフトウェア99bを復号できるようにすることも可能である。

【0018】

また、本発明の第4の態様では、ライセンスによって実行が制限されたソフトウェアを実行する処理装置において、装置識別情報が固定的に記録された記録媒体と、動作許可対象装置を特定する許可対象装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報が格納されたハードウェアキーが装着されたとき、前記ハードウェアキーから前記着脱キー情報を読み取るハードウェアキー接続手段と、暗号化された状態の前記ソフトウェアを提供するソフトウェア提供サーバから、前記ソフトウェアを復号するためのソフトウェア復号キーが暗号化された状態で含まれたライセンス情報を取得するライセンス取得手段と、前記ソフトウェア復号キーを前記着脱キー固有暗号キーで復号するソフトウェアキー復号手段と、

前記ハードウェアキー接続手段に接続された前記ハードウェアキーに含まれる前記許可対象識別情報と前記記録媒体に記録された装置識別情報との同一性を判定する識別情報判定手段と、前記識別情報判定手段により、同一であると判定された場合には、前記ソフトウェアキー復号手段で復号された前記ソフトウェア復号キーで、暗号化された状態の前記ソフトウェアを復号するソフトウェア復号手段と、を有することを特徴とする処理装置が提供される。

#### 【0019】

このような処理装置によれば、取得したライセンス情報のソフトウェア復号キーを暗号化したときの着脱キー固有暗号キーが格納されたハードウェアキーが装着され、且つ、そのハードウェアキーに格納された装置識別情報と記録媒体に記録された装置識別情報とが同一の場合にのみ、ソフトウェアが復号される。

#### 【0020】

本発明の第5の態様では、ライセンスによって実行が制限されたソフトウェアの実行状況を管理するソフトウェア実行管理装置において、装置識別情報が固定的に記録された記録媒体と、動作許可対象装置を特定する許可対象装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報が格納されたハードウェアキーが装着されたとき、前記ハードウェアキーから前記着脱キー情報を読み取るハードウェアキー接続手段と、前記ソフトウェアを提供するソフトウェア提供サーバから、前記ソフトウェアを復号するための暗号化された状態のソフトウェア復号キーと、同時実行可能なコンピュータ数とが含まれたライセンス情報を取得するライセンス取得手段と、前記ソフトウェア復号キーを前記着脱キー固有暗号キーで復号するソフトウェアキー復号手段と、ネットワークを介して接続されたコンピュータのうち前記ソフトウェアを実行している実行コンピュータ数を監視し、前記同時実行可能なコンピュータ数以下の数の前記コンピュータに対して、前記ソフトウェアキー復号手段で復号された前記ソフトウェア復号キーを渡す復号キー管理手段と、を有することを特徴とするソフトウェア実行管理装置が提供される。

#### 【0021】

本発明の第6の態様では、ソフトウェアの実行ライセンスを発行するためのラ

イセンス発行方法において、前記ソフトウェアの暗号化のための暗号キー生成要求に応じて、ソフトウェア暗号キーと、前記ソフトウェア暗号キーで暗号化される前記ソフトウェアを復号するためのソフトウェア復号キーとを生成し、前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含むライセンス発行要求に応じて、前記装置識別情報を暗号キーとして前記ソフトウェア復号キーを暗号化し、暗号化された前記ソフトウェア復号キーを含むソフトウェアライセンスを出力する、ことを特徴とするライセンス発行方法が提供される。

#### 【0022】

本発明の第7の態様では、ソフトウェアの実行ライセンスを発行するためのライセンス発行方法において、前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含む着脱キー情報生成要求に回答して、前記装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報を生成し、生成した前記着脱キー情報を、前記処理装置に着脱可能なハードウェアキーに記録し、前記ソフトウェアのライセンス発行要求に応じて、暗号化された状態で提供される前記ソフトウェアを復号するためのソフトウェア復号キーを前記着脱キー固有暗号キーで暗号化して、暗号化された前記ソフトウェア復号キーを含むライセンス情報を出力する、ことを特徴とするライセンス発行方法が提供される。

#### 【0023】

本発明の第8の態様では、ソフトウェアの実行ライセンスを発行するためのライセンス発行プログラムにおいて、コンピュータに、前記ソフトウェアの暗号化のための暗号キー生成要求に応じて、ソフトウェア暗号キーと、前記ソフトウェア暗号キーで暗号化される前記ソフトウェアを復号するためのソフトウェア復号キーとを生成し、前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含むライセンス発行要求に応じて、前記装置識別情報を暗号キーとして前記ソフトウェア復号キーを暗号化し、暗号化された前記ソフトウェア復号キーを含むソフトウェアライセンスを出力する、処理を実行させることを特徴とするライセンス発行プログラムが提供される。

**【0024】**

本発明の第9の態様では、ソフトウェアの実行ライセンスを発行するためのライセンス発行プログラムにおいて、コンピュータに、前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含む着脱キー情報生成要求に応答して、前記装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報を生成し、生成した前記着脱キー情報を、前記処理装置に着脱可能なハードウェアキーに記録し、前記ソフトウェアのライセンス発行要求に応じて、暗号化された状態で提供される前記ソフトウェアを復号するためのソフトウェア復号キーを前記着脱キー固有暗号キーで暗号化して、暗号化された前記ソフトウェア復号キーを含むライセンス情報を出力する、処理を実行させることを特徴とするライセンス発行プログラムが提供される。

**【0025】****【発明の実施の形態】**

以下、本発明の実施の形態を図面を参照して説明する。

**【第1の実施の形態】**

まず、実施の形態に適用される発明の概要について説明し、その後、実施の形態の具体的な内容を説明する。

**【0026】**

図1は、第1の実施の形態に適用される発明の概念図である。第1の実施の形態は、ハードウェア固有の装置識別情報4bを用いて、ソフトウェア6aのライセンス管理を行うものである。そのために、以下の機能が提供される。

**【0027】**

ソフトウェア暗号キー生成手段1は、ソフトウェア6aの暗号化のための暗号キー生成要求に応じて、ソフトウェア暗号キー5aと、ソフトウェア暗号キー5aで暗号化されたソフトウェア6bを復号するためのソフトウェア復号キー5bとを生成する。

**【0028】**

ライセンス発行手段2は、ソフトウェア6aの動作許可対象である処理装置4内の記録媒体4aに固定的に記録された装置識別情報4bを含むライセンス発行

要求に応じて、装置識別情報 4 b でソフトウェア復号キー 5 b を暗号化し、暗号化されたソフトウェア復号キーを含むソフトウェアライセンス 5 c を出力する。出力されたソフトウェアライセンス 5 c は、処理装置 4 に渡される。

**【0029】**

ソフトウェア暗号化手段 3 は、ソフトウェア暗号キー 5 a を用いて、ソフトウェア 6 a を暗号化する。暗号化されたソフトウェア 6 b は、処理装置 4 に渡される。

**【0030】**

処理装置 4 には、記録媒体 4 a、復号キー復号手段 4 c、およびソフトウェア復号手段 4 d が設けられている。記録媒体 4 a は、装置識別情報 4 b が固定的に記録されている。復号キー復号手段 4 c は、暗号化された状態のソフトウェア復号キーを含むソフトウェアライセンス 5 c を受け取ると、記録媒体 4 a に記録された装置識別情報 4 b を復号キーとしてソフトウェア復号キー 5 d を復号する。ソフトウェア復号手段 4 d は、ソフトウェア提供サーバから暗号化された状態のソフトウェア 6 b を受け取ると、復号キー復号手段 4 c で復号されたソフトウェア復号キー 5 d を復号キーとしてソフトウェア 6 b を復号する。これにより、暗号化されているソフトウェア 6 c が再現される。

**【0031】**

このようなライセンス発行サーバによれば、ソフトウェア復号キー 5 b を装置識別情報 4 b で暗号化しているため、その装置識別情報 4 b が固定的に記録された処理装置 4 でのみ暗号化されたソフトウェア 6 b を復号することが可能となる。しかも、装置識別情報 4 b は、処理装置 4 の記録媒体 4 a（たとえば所定のアドレス空間が割り当てられた読み取り専用の半導体メモリ）に固定的に記録されているため、ソフトウェア的な操作で複製の作成や改竄等を行うのは困難である。その結果、ソフトウェア 6 a の不正使用が防止できる。

**【0032】**

以下、第 1 の実施の形態に係るシステムを詳細に説明する。

図 2 は、第 1 の実施の形態のシステム構成例を示す図である。第 1 の実施の形態では、ソフトウェアの開発や販売を行うソフトウェア提供者 21、ソフトウェ

アのライセンス発行を代行するライセンス発行局 22、および販売されたソフトウェアを利用する利用者 23との間で、ソフトウェアの取引に関する手続きが行われる。

**【0033】**

ソフトウェア提供者 21は、ソフトウェア提供サーバ 100を所持している。ソフトウェア提供サーバ 100は、ネットワーク等を介してソフトウェアを配付するためのコンピュータである。

**【0034】**

ライセンス発行局 22は、ライセンス発行サーバ 200を所持している。ライセンス発行サーバ 200は、ソフトウェア提供サーバ 100とネットワークを介して接続されている。ライセンス発行サーバ 200は、ソフトウェア提供サーバ 100からの要求に応じて、利用者に引き渡すソフトウェアの暗号キーの生成や、利用者毎のソフトウェアライセンスキーの発行を行う。詳細には、ライセンス発行サーバ 200は、ソフトウェア提供サーバ 100からの暗号キー要求に応じてソフトウェアの暗号キーを生成し、利用者毎のソフトウェア要求に応じてソフトウェアライセンスキーを生成する。

**【0035】**

生成されたソフトウェアライセンスキーと暗号キーとは、ネットワークあるいは可搬型の記録媒体（メモリカードなど）などの情報伝達媒体を介して、ソフトウェア提供サーバ 100に渡される。

**【0036】**

利用者 23は、処理装置 300を所持している。処理装置 300は、ネットワークを介してソフトウェア提供サーバ 100に接続されている。処理装置 300は、利用者 23からの操作入力に応じて、ソフトウェア要求をソフトウェア提供サーバ 100に送信する。ソフトウェア提供サーバ 100から暗号化されたソフトウェアと暗号化されたソフトウェアライセンスキーとを受け取ると、処理装置 300は、ソフトウェアライセンスキーで許可されている範囲内でソフトウェアを実行する。

**【0037】**

図3は、本発明の実施の形態に用いるソフトウェア提供サーバのハードウェア構成例を示す図である。ソフトウェア提供サーバ100は、CPU(Central Processing Unit)101によって装置全体が制御されている。CPU101には、バス107を介してRAM(Random Access Memory)102、ハードディスクドライブ(HDD:Hard Disk Drive)103、グラフィック処理装置104、入力インタフェース105、および通信インタフェース106が接続されている。

#### 【0038】

RAM102には、CPU101に実行させるOS(Operating System)のプログラムやアプリケーションプログラムの少なくとも一部が一時的に格納される。また、RAM102には、CPU101による処理に必要な各種データが格納される。HDD103には、OSやアプリケーションプログラムが格納される。

#### 【0039】

グラフィック処理装置104には、モニタ11が接続されている。グラフィック処理装置104は、CPU101からの命令に従って、画像をモニタ11の画面に表示させる。入力インタフェース105には、キーボード12とマウス13とが接続されている。入力インタフェース105は、キーボード12やマウス13から送られてくる信号を、バス107を介してCPU101に送信する。

#### 【0040】

通信インタフェース106は、ネットワーク10に接続されている。通信インタフェース106は、ネットワーク10を介して、他のコンピュータとの間でデータの送受信を行う。

#### 【0041】

以上のようなハードウェア構成によって、本実施の形態の処理機能を実現することができる。なお、図3には、ソフトウェア提供サーバ100のハードウェア構成例を示したが、ライセンス発行サーバ200や処理装置300も同様のハードウェア構成で実現することが出来る。

#### 【0042】

次に、第1の実施の形態における各装置の処理機能について説明する。

図4は、第1の実施の形態に係るソフトウェアライセンス管理システムの機能

ブロック図である。図4には、ソフトウェア提供サーバ100、ライセンス発行サーバ200、および処理装置300それぞれが有する処理機能で示されている。

#### 【0043】

また、図4において、暗号化された情報を  $a[b]$  の形式で表現する。このとき、 $a$  は、暗号化に用いたキー（暗号鍵）である。 $b$  は、暗号化されたデータである。

#### 【0044】

ソフトウェア提供サーバ100は、暗号キー要求部110、ソフトウェア暗号化部120、ソフトウェア要求受付部130、ソフトウェア提供部140、およびソフトウェアライセンス提供部150を有している。

#### 【0045】

暗号キー要求部110は、ソフトウェア提供者21からのソフトウェア ( $s1$ ) 31の暗号化を指示する操作入力に応答して、ソフトウェア暗号キー生成要求をライセンス発行サーバ200に対して出力する。なお、ネットワークを介さずに、郵送等によりソフトウェア暗号キー生成依頼をライセンス発行局22に渡してもよい。その場合、ライセンス発行局22のオペレータが、ソフトウェア暗号キー生成要求をライセンス発行サーバ200に操作入力する。また、ソフトウェア暗号キー生成要求の内容を可搬型の記録媒体に格納し、その記録媒体をライセンス発行局22に郵送してもよい。この場合、ライセンス発行局22のオペレータが、その記録媒体をライセンス発行サーバ200に挿入し、ソフトウェア暗号キー生成要求をライセンス発行サーバ200に入力する。

#### 【0046】

ソフトウェア暗号化部120は、ソフトウェア暗号キー生成要求に応じてライセンス発行サーバ200から返されたソフトウェア暗号キー（公開-key1）41を受け取る。このソフトウェア暗号キー（公開-key1）41は、公開鍵である。そして、ソフトウェア暗号化部120は、受け取ったソフトウェア暗号キー（公開-key1）41を用いて、ソフトウェア31を暗号化する。これにより、暗号化済ソフトウェア（公開-key1[ $s1$ ]) 32が生成される。暗号化済ソフトウェア（

公開-key1[s1]) 32は、ソフトウェア提供サーバ100内のHDD103等に格納される。

#### 【0047】

ソフトウェア要求受付部130は、処理装置300からのソフトウェア要求を受け取る。ソフトウェア要求を受け取ったソフトウェア要求受付部130は、まず、利用者23が正当にソフトウェア31の購入手続きを行っていることを確認する。たとえば、ソフトウェア31の購入者に通知しているパスワード等の入力によるユーザ認証を行う。

#### 【0048】

正当な購入者であることを確認したら、ソフトウェア要求受付部130は、ソフトウェア提供部140に対してソフトウェアの提供を指示する。また、ソフトウェア要求受付部130は、ライセンス発行サーバ200に対して、ソフトウェアライセンスキー要求を出力する。

#### 【0049】

ソフトウェア提供部140は、ソフトウェア要求受付部130からソフトウェア提供指示を受け取ると、ソフトウェア提供サーバ100内に保持されている暗号化済ソフトウェア（公開-key1[s1]) 32の複製を配信用の暗号化済ソフトウェア33とし、処理装置300に対してネットワークを介して送信する。なお、暗号化済ソフトウェア33を郵送で利用者23に渡してもよい。その場合、ソフトウェア提供部140は、暗号化済ソフトウェア33を可搬型記録媒体（たとえば、メモリカード）に格納する。そして、ソフトウェア提供者21のオペレータが、暗号化済ソフトウェア33が格納された可搬型記録媒体を利用者23に送付する。

#### 【0050】

ソフトウェアライセンス提供部150は、ソフトウェアライセンスキー要求に応じてライセンス発行サーバ200から返されたソフトウェアライセンスキー（idl[秘密-key1]) 44を受け取る。そして、ソフトウェアライセンス提供部150は、ソフトウェアライセンスキー（idl[秘密-key1]) 45を処理装置300へネットワークを介して送信する。なお、ソフトウェアライセンスキー（idl[秘密

-key1]) 45を郵送等によって利用者23に渡してもよい。その場合、ソフトウェアライセンス提供部150は、ソフトウェアライセンスキー(id1[秘密-key1]) 45を可搬型記録媒体に格納する。

#### 【0051】

ライセンス発行サーバ200は、ソフトウェア暗号キー生成部210とソフトウェアライセンスキー生成部220とを有している。

ソフトウェア暗号キー生成部210は、ソフトウェア提供サーバ100の暗号キー要求部110から出されたソフトウェア暗号キー生成要求を受け取る。そして、ソフトウェア暗号キー生成部210は、ソフトウェア暗号キー生成要求に回答して、ソフトウェア暗号キー(公開-key1) 41とソフトウェア復号キー(秘密-key1) 42とを生成する。ソフトウェア暗号キー(公開-key1) 41を暗号キーとして暗号化したデータは、ソフトウェア復号キー(秘密-key1) 42を復号キーとして復号した場合にのみ、元通りに復元することが出来る。なお、ソフトウェア暗号キー(公開-key1) 41は公開鍵であるが、ソフトウェア復号キー(秘密-key1) 42は秘密鍵である。

#### 【0052】

ソフトウェア暗号キー生成部210は、ソフトウェア暗号キー(公開-key1) 41をソフトウェア提供サーバ100にネットワークを介して送信する。なお、ソフトウェア暗号キー(公開-key1) 41を可搬型記録媒体に格納し、郵送等によりソフトウェア提供者21に渡すことも出来る。また、ソフトウェア暗号キー生成部210は、ソフトウェア復号キー(秘密-key1) 42をライセンス発行サーバ200内のHDD等に格納する。

#### 【0053】

ソフトウェアライセンスキー生成部220は、ソフトウェア提供サーバ100のソフトウェア要求受付部130から送られるソフトウェアライセンスキー要求を受け取る。すると、ソフトウェアライセンスキー生成部220は、ソフトウェアライセンスキー要求から装置識別情報(id1) 43を取り出す。そして、ソフトウェアライセンスキー生成部220は、ソフトウェアライセンスキー要求に回答して、ソフトウェア復号キー(秘密-key1) 42を装置識別情報(id1) 43で暗号

化し、ソフトウェアライセンスキー (idl[秘密-key1]) 4 4 を生成する。さらに、ソフトウェアライセンスキー生成部 2 2 0 は、生成したソフトウェアライセンスキー (idl[秘密-key1]) 4 4 をソフトウェア提供サーバ 1 0 0 にネットワークを介して送信する。なお、ソフトウェアライセンスキー (idl[秘密-key1]) 4 4 を可搬型記録媒体に格納し、郵送等によりソフトウェア提供者 2 1 に渡してもよい。

#### 【0 0 5 4】

処理装置 3 0 0 は、識別情報記憶部 3 1 0、ソフトウェア要求部 3 2 0、ソフトウェアライセンスキー復号部 3 3 0、ソフトウェア復号部 3 4 0 およびソフトウェア実行部 3 5 0 を有している。

#### 【0 0 5 5】

識別情報記憶部 3 1 0 は、処理装置 3 0 0 に内蔵された記録媒体（たとえば、ROM等の半導体メモリ）であり、処理装置 3 0 0 を一意に識別可能な装置識別情報 4 3 が予め記録されている。この装置識別情報 4 3 は、処理装置の製造メーカーにおいて書き込まれ、利用者 2 3 がその内容を変更することはできない。

#### 【0 0 5 6】

ソフトウェア要求部 3 2 0 は、利用者からの操作入力等に基づいて、ソフトウェア要求をソフトウェア提供サーバ 1 0 0 にネットワークを介して送信する。なお、ソフトウェア要求部 3 2 0 は、ソフトウェア要求を送信する際には、識別情報記憶部 3 1 0 から装置識別情報 4 3 を取得し、その装置識別情報 4 3 をソフトウェア要求に含める。また、ソフトウェア要求を郵送等によりソフトウェア提供者 2 1 に渡す場合には、ソフトウェア要求部 3 2 0 は、装置識別情報 4 3 を含むソフトウェア要求を可搬型記録媒体に格納する。

#### 【0 0 5 7】

ソフトウェアライセンスキー復号部 3 3 0 は、ソフトウェア提供サーバ 1 0 0 からネットワークを介して送信されたソフトウェアライセンスキー (idl[秘密-key1]) 4 5 を受け取る。なお、ソフトウェアライセンスキー (idl[秘密-key1]) 4 5 が郵送で渡される場合、ソフトウェアライセンスキー (idl[秘密-key1]) 4 5 が格納された可搬型記録媒体が、利用者 2 3 によって処理装置 3 0 0 に挿入さ

れる。ソフトウェアライセンスキー復号部 3 3 0 は、挿入された可搬型記録媒体からソフトウェアライセンスキー (idl[秘密-key1]) 4 5 を読み出す。

#### 【0 0 5 8】

ソフトウェアライセンスキー (idl[秘密-key1]) 4 5 を取得したソフトウェアライセンスキー復号部 3 3 0 は、識別情報記憶部 3 1 0 から装置識別情報(idl)を取得する。そして、ソフトウェアライセンスキー復号部 3 3 0 は、装置識別情報(idl)を用いて、ソフトウェアライセンスキー (idl[秘密-key1]) 4 5 を復号する。これにより、ソフトウェア復号キー (秘密-key1) 4 6 が復元される。復元されたソフトウェア復号キー (秘密-key1) 4 6 は、ソフトウェア復号部 3 4 0 に渡される。

#### 【0 0 5 9】

ソフトウェア復号部 3 4 0 は、ソフトウェア提供サーバ 1 0 0 から送られた暗号化済ソフトウェア (公開-key1[s1]) 3 3 を受け取る。そして、ソフトウェア復号部 3 4 0 は、ソフトウェア復号キー (秘密-key1) 4 6 を用いて、暗号化済ソフトウェア (公開-key1[s1]) 3 3 を復号し、ソフトウェア(s1) 3 4 を復元する。

#### 【0 0 6 0】

ソフトウェア実行部 3 5 0 は、復元されたソフトウェア(s1) 3 4 を実行する。

以上のような構成のライセンス管理システムにおいて、以下の様な手順でライセンスが与えられた利用者に対してソフトウェアが提供される。なお、ソフトウェアの提供は、開発されたソフトウェアの暗号化処理と、ソフトウェア提供処理とに分かれる。

#### 【0 0 6 1】

図 5 は、第 1 の実施の形態におけるソフトウェア暗号化処理を示すシーケンス図である。以下、図 5 に示す処理をステップ番号に沿って説明する。

[ステップ S 1 1] ソフトウェア提供サーバ 1 0 0 に対して、ソフトウェア提供者 2 1 からソフトウェア(s1) 3 1 の暗号化指示が入力されると、暗号キー要求部 1 1 0 からライセンス発行サーバ 2 0 0 に対して、ソフトウェア暗号キー生成要求が送信される。なお、郵送等によりソフトウェア暗号キー生成依頼を、ソフ

トウェア発行局 22 に渡すこともできる。

#### 【0062】

[ステップ S12] ライセンス発行サーバ 200 では、ソフトウェア暗号キー生成要求に応答して、ソフトウェア暗号キー生成部 210 が暗号キーを生成する。具体的には、ソフトウェア暗号キー生成部 210 は、ソフトウェア暗号キー（公開-key1）41 とソフトウェア復号キー（秘密-key1）42 とを生成する。

#### 【0063】

[ステップ S13] 次に、ソフトウェア暗号キー生成部 210 は、ソフトウェア暗号キー（公開-key1）41 をソフトウェア提供サーバ 100 に対して送信する。なお、郵送等により、ソフトウェア暗号キー（公開-key1）41 をソフトウェア提供者 21 に渡すこともできる。

#### 【0064】

[ステップ S14] さらに、ソフトウェア暗号キー生成部 210 は、ソフトウェア復号キー（秘密-key1）42 を記憶する。

[ステップ S15] ソフトウェア提供サーバ 100 では、ソフトウェア暗号化部 120 が、ソフトウェア暗号キー（公開-key1）41 を用いて、ソフトウェア(s1)31 を暗号化する。これにより、暗号化済ソフトウェア（公開-key1[s1]）32 が生成される。

#### 【0065】

[ステップ S16] そして、ソフトウェア暗号化部 120 は、暗号化済ソフトウェア（公開-key1[s1]）32 を記憶する。

このようにして、ソフトウェア提供者が開発したソフトウェア(s1)31 が暗号化され、暗号化済ソフトウェア（公開-key1[s1]）32 がソフトウェア提供サーバ 100 内に格納される。このとき、暗号化済ソフトウェア（公開-key1[s1]）32 を復号するためのソフトウェア復号キー（秘密-key1）42 は、ライセンス発行サーバ 200 内に格納される。

#### 【0066】

このような状況下で、利用者 23 がソフトウェア提供者 21 からのソフトウェア 31 の購入申し込みを行う。この購入申し込みは、たとえば、インターネット

等を介したオンライン取引で行うことができる。また、電話や店頭における直接取引により、ソフトウェアの購入申し込みを行うこともできる。購入申し込み手続きが完了すると、ソフトウェア引き渡し処理が行われる。

#### 【0067】

図6は、第1の実施の形態におけるソフトウェア提供処理を示すシーケンス図である。以下、図6に示す処理をステップ番号に沿って説明する。

[ステップS21] 利用者23により処理装置300に対してソフトウェア(s1)31の取得を指示する操作入力が行われると、ソフトウェア要求部320がソフトウェア提供サーバ100に対してソフトウェア要求を送信する。このとき、ソフトウェア要求には、識別情報記憶部310から取得した装置識別情報(id1)が含まれる。また、利用者23が正当にソフトウェア31の購入手続きを行った者であることを示す認証情報を、ソフトウェア要求に含めることもできる。

#### 【0068】

なお、装置識別情報(id1)を含むソフトウェア要求が格納された可搬型記録媒体を、郵送あるいは直接の手渡しによりソフトウェア提供者21に渡すこともできる。

#### 【0069】

[ステップS22] ソフトウェア提供サーバ100では、ソフトウェア要求を受け取ると、ソフトウェア要求受付部130が、ソフトウェア(s1)31の購入手続きを正当に行った者からの要求であることを確認する。正当な購入者であることを確認すると、ソフトウェア要求受付部130からソフトウェア提供部140へソフトウェア提供指示が出される。

#### 【0070】

[ステップS23] ソフトウェア提供指示を受け取ったソフトウェア提供部140は、暗号化済ソフトウェア(公開-key1[s1])32を処理装置300に送信する。なお、暗号化済ソフトウェア(公開-key1[s1])32を可搬型記録媒体に格納し、郵送等により利用者23に渡すこともできる。

#### 【0071】

[ステップS24] さらにソフトウェア要求受付部130は、ライセンス発行

サーバ200に対して、ソフトウェアライセンスキー要求を送信する。ソフトウェアライセンスキー要求には、装置識別情報(id1)43が含まれる。なお、ソフトウェアライセンスキー要求を記録媒体に格納し、郵送等によりライセンス発行局22に渡すこともできる。

#### 【0072】

なお、ステップS23とステップS24との処理は、順番が逆でもよい。

〔ステップS25〕ソフトウェアライセンスキー要求を受け取ったライセンス発行サーバ200では、ソフトウェアライセンスキー生成部220がソフトウェア復号キー（秘密-key1）42を、装置識別情報(id1)43を暗号キーとして利用して暗号化する。これにより、ソフトウェアライセンスキー（id1[秘密-key1]）44が生成される。

#### 【0073】

〔ステップS26〕ソフトウェアライセンスキー生成部220は、生成したソフトウェアライセンスキー（id1[秘密-key1]）44をソフトウェア提供サーバ100に送信する。なお、ソフトウェアライセンスキー（id1[秘密-key1]）44を可搬型記録媒体に格納し、郵送等によりソフトウェア提供者21に渡すこともできる。

#### 【0074】

〔ステップS27〕ソフトウェア提供サーバ100では、ソフトウェアライセンス提供部150がライセンス発行サーバ200から送られたソフトウェアライセンスキー（id1[秘密-key1]）44を受け取る。そして、ソフトウェアライセンス提供部150は、ソフトウェアライセンスキー（id1[秘密-key1]）44を処理装置300に送信する。なお、ソフトウェアライセンスキー（id1[秘密-key1]）44を可搬型記録媒体に格納し、郵送等により利用者23に渡すこともできる。

#### 【0075】

〔ステップS28〕処理装置300では、ソフトウェアライセンスキー復号部330が、識別情報記憶部310に格納されている装置識別情報(id1)43を復号キーとして用い、ソフトウェアライセンスキー（id1[秘密-key1]）44を復号する。これにより、ソフトウェア復号キー（秘密-key1）46が生成される。生

成されたソフトウェア復号キー（秘密-key1）46は、ソフトウェア復号部340に渡される。

【0076】

〔ステップS29〕ソフトウェア復号部340は、ソフトウェア復号キー（秘密-key1）46を復号キーとして用い、暗号化済ソフトウェア（公開-key1[s1]）33を復号する。これにより、平文のソフトウェア(s1)34が生成される。

【0077】

〔ステップS30〕ソフトウェア実行部350が、ソフトウェア(s1)34を実行する。

このようにして、ソフトウェアロック機構提供者（ライセンス発行局22）からソフトウェア提供者21にソフトウェア暗号キー41と、利用者23からの要求ごとのソフトウェアライセンスキー44とを発行することで、以下のような効果が得られる。

【0078】

第1の実施の形態では、ソフトウェア31を暗号化して提供するとともに、利用者自身が変更できない装置識別情報43を用いてソフトウェア復号キー42を暗号化して、処理装置に提供するようにした。そのため、ソフトウェアの不正使用を強固に防止することができる。

【0079】

すなわち、ソフトウェア31が暗号化されて提供されるため、ソフトウェア31の復号処理を行わない限り、ソフトウェア31を実行することも、その処理内容を解析することも出来ない。従って、提供されるソフトウェア31を改竄することによる不正使用を防ぐことが出来る。

【0080】

しかも、復号には、工場出荷時に設定され、利用者による変更ができない装置識別情報43が必要である。この装置識別情報43を用いてソフトウェアライセンスキー45を復号しなければならないため、ソフトウェア31を他の装置で実行することができない。したがって、OSによって定義されるマシン識別コード等を用いた場合に比べ、不正使用が困難となりソフトウェア31の保護が強化さ

れる。

#### 【0081】

また、ソフトウェア提供者 21 はソフトウェア 31 自体を第三者機関であるライセンス発行局に持ち込むことなく（効率、著作権保護）ソフトウェアロック（ソフトウェア保護）が利用できる。これにより、ソフトウェア 31 のバージョンアップ等が行われた際にも、予め提供されたソフトウェア暗号キー 41 で暗号化すればよく、ライセンスの再発行等の手続きは不要となる。したがって、ソフトウェア提供者 21 に係るソフトウェア保護のための作業負担を軽減することが出来る。

#### 【0082】

さらに、ソフトウェアロック機構提供者（ライセンス発行局 22）によってソフトウェア復号キー 42 が管理されているため、ライセンス発行サーバ 200 に対してセキュリティの高い運用を行えば、ソフトウェア復号キー 42 の第三者による不正入手を防止できる。たとえば、ライセンス発行サーバ 200 に関しては、システム運用状況を監視し、不正なアクセスに対しては、セキュリティ専門の技術者が迅速に対応できるようにする。これにより、ソフトウェア提供サーバ 100 において必要以上にセキュリティの高い運用を行わずに済み、ソフトウェア提供者 21 の負担が軽減される。

#### 【0083】

なお、ソフトウェア提供サーバ 100 におけるソフトウェア 31 は、暗号化をするときにのみソフトウェア提供サーバ 100 からアクセス可能な状態とし、暗号化後はソフトウェア提供サーバ 100 からアクセスできないようにする。これにより、ソフトウェア提供サーバ 100 の運用中に不正にアクセスしても、暗号化前のソフトウェア 31 を取得することはできない。

#### 【0084】

ここで、ソフトウェアロック機構提供者（ライセンス発行局 22）は、ソフトウェア復号キー 42 の秘密保持サービス提供の対価を、ソフトウェア提供者 21 から徴収しても良い。その場合、たとえば、ソフトウェア提供者 21 がソフトウェアロック（ソフトウェア保護）を利用するごと（ソフトウェアライセンスキー

44の提供を受ける毎)に対価を得ることができる。

【0085】

また、ソフトウェア暗号キー生成部210で、ソフトウェアごとに公開キーと秘密キーのペアを生成し、公開キーをソフトウェア開発者に送付、ソフトウェアライセンスキーとして秘密キーを利用するため、ソフトウェア提供者21によるライセンスの無断発行ができない。これは、ソフトウェア提供者21によるソフトウェア31の販売数量を、第三者機関によって客観的に把握できるという利点がある。

【0086】

たとえば、開発されたソフトウェア31の一部の機能に、他の特許技術(動画圧縮技術など)が使用されている場合がある。この場合、他の特許技術の特許権者から特許技術の実施許諾を受けることで、ソフトウェア31を販売することが出来る。ここで、ソフトウェア31の販売数量に応じた実施料を支払う契約の場合、販売数量を正しく算定しなければならない。そこで、第1の実施の形態に示すように、第三者機関であるライセンス発行局22によってライセンス発行数を管理していれば、実際の販売数量の算定が正しく行われる。その結果、実施許諾者(ライセンサー)と実施権者(ライセンシー)との間で、実施権料の支払額に関して疑義が生じることがなくなる。

【0087】

さらに、ソフトウェアベンダ(ソフトウェア提供者21)は、ソフトウェア保護のためにソフトウェアを暗号化しておくのみでよい。すなわち、アプリケーションソフトウェア保護のためのソフトウェアロジックをプログラム中に追加しなくてもよい。その結果、ソフトウェアの開発効率が向上する。

【0088】

次に、第1の実施の形態に係るライセンス管理システムの応用例について説明する。

ソフトウェア要求部320からの出力されるソフトウェア要求に、ソフトウェア利用条件(ソフトウェア実行数や実行範囲の情報)を示す情報を含めることで、ソフトウェアライセンスキー44内にソフトウェア利用条件を設定することが

できる。

#### 【0089】

この場合、ソフトウェア要求受付部130は、ソフトウェア要求に含まれるソフトウェア利用条件に応じた料金支払い手続きが完了していることを確認後、ライセンス発行サーバ200に対して、ソフトウェア利用条件を含むソフトウェアライセンスキー要求をネットワーク経由で送信する。なお、ソフトウェアライセンスキー要求を可搬型記録媒体に格納し、郵送等でライセンス発行局22に渡すこともできる。

#### 【0090】

ライセンス発行サーバ200内のソフトウェアライセンスキー生成部220は、ソフトウェア利用条件とソフトウェア復号キー42とを合わせて暗号化し、ソフトウェアライセンスキー44を生成する。

#### 【0091】

このようなソフトウェアライセンスキー44が処理装置300のソフトウェアライセンスキー復号部330で復号されると、ソフトウェア復号キー46と共に、ソフトウェア利用条件が復元される。ソフトウェア実行部350は、ソフトウェア使用条件を参照し、ソフトウェア利用条件で許可された機能しか実行しない。

#### 【0092】

このように、ソフトウェア利用条件の情報も含めてソフトウェアライセンスキー44を生成することで、ソフトウェア実行時に、許諾したソフトウェア利用条件（ソフトウェア価格）の範囲に動作を制約することもできる。

#### 【0093】

ソフトウェア暗号化部120において、ソフトウェア31の一部のみを暗号化することもできる。たとえば、ソフトウェア提供者21がソフトウェア構成部分の暗号化範囲（保護したい重要なファイル等）を選択すると、ソフトウェア暗号化部120は選択された範囲のみを暗号化すると共に、選択した範囲の情報（ファイル一覧等）を暗号化済ソフトウェア32に含める。ソフトウェア復号部340は、選択された範囲を復号する。このようにして、ソフトウェア31の一部の

みを暗号化して提供することで、ソフトウェア復号処理の時間を短縮することができる。

#### 【0094】

なお、上記の例では、ライセンス発行サーバ200とソフトウェア提供サーバ100との機能を分けているが、1つのサーバ（たとえば、ソフトウェア提供サーバ）でソフトウェアの提供とライセンスの発行とを行ってもよい。

#### 【0095】

##### [第2の実施の形態]

次に、第2の実施の形態について説明する。第2の実施の形態は、処理装置の識別情報を高い耐タンパ性（物理的な攻撃に対する耐性）を有したハードウェア（以下、ハードウェアキーと呼ぶ）に格納して、ユーザに提供するものである。ユーザは、ハードウェアキーに格納された識別情報と合致する装置識別情報を有する装置でなければ、ソフトウェアを実行することが出来ない。

#### 【0096】

図7は、第2の実施の形態に適用される発明の概念図である。ライセンス管理システムは、着脱キー情報発行手段91、ライセンス発行手段92、ソフトウェア暗号化手段93、および処理装置94で構成される。

#### 【0097】

着脱キー情報発行手段91は、着脱キー情報生成要求に応答して、装置識別情報91bと着脱キー固有暗号キー91cとを含む着脱キー情報91aを生成する。なお、着脱キー情報生成要求には、ソフトウェア99aの動作許可対象である処理装置94内の記録媒体94aに固定的に記録された装置識別情報91bが含まれる。着脱キー情報発行手段91は、生成した着脱キー情報91aを、処理装置94に着脱可能なハードウェアキー96に記録する。ハードウェアキー96は、処理装置94の利用者に渡される。

#### 【0098】

ライセンス発行手段92は、ソフトウェアのライセンス発行要求に応じて、ソフトウェア復号キー98aを着脱キー固有暗号キー91cで暗号化して、暗号化されたソフトウェア復号キー98cを含むライセンス情報98bを出力する。な

お、ソフトウェア復号キー 98 a は、暗号化されたソフトウェア 99 b を復号するためのキー情報である。出力されたライセンス情報 98 b は、処理装置 94 に渡される。

#### 【0099】

ソフトウェア暗号化手段 93 は、ソフトウェア暗号キー 98 を用いて、ソフトウェア 99 a を暗号化する。そして、暗号化されたソフトウェア 99 b を処理装置 94 に渡す。

#### 【0100】

処理装置 94 は、記録媒体 94 a、ライセンス情報復号手段 94 b、識別情報判定手段 94 c、ソフトウェア復号手段 94 d、およびハードウェアキー接続手段 94 e を有している。

#### 【0101】

記録媒体 94 a は、装置識別情報 91 b が固定的に記録されている。ハードウェアキー接続手段 94 e は、ハードウェアキー 96 が装着されたとき、ハードウェアキー 96 から着脱キー情報 91 a を読み取る。ライセンス情報復号手段 94 b は、ソフトウェア 99 a を復号するためのソフトウェア復号キー 98 c が暗号化された状態で含まれたライセンス情報 98 b が入力されると、ソフトウェア復号キー 98 c を着脱キー固有暗号キー 91 c で復号する。識別情報判定手段 94 c は、装着されたハードウェアキー 96 に含まれる装置識別情報 91 b と前記記録媒体 94 a に記録された装置識別情報との同一性を判定する。ソフトウェア復号手段 94 d は、識別情報判定手段 94 c により、装置識別情報が同一であると判定された場合には、ソフトウェアキー復号手段 94 b で復号されたソフトウェア復号キー 98 a で、暗号化された状態のソフトウェア 99 b を復号し、暗号化されていないソフトウェア 99 c を生成する。

#### 【0102】

このようなライセンス管理システムによれば、正しいハードウェアキー 96 が装着された処理装置 94 に限りライセンス情報 98 b を復号し、暗号化された状態のソフトウェア 99 b を復号することができる。しかも、装置識別情報 91 b がハードウェアキー 96 に格納されていることにより、装置識別情報が合致する

処理装置でのみソフトウェア 99b を復号できる。

#### 【0103】

ところで、ソフトウェアの利用者には企業も含まれる。企業内のコンピュータシステムを動作させるには、多種多様のソフトウェアが利用される。たとえば、社内のイントラネットを構築する場合、ファイアウォール、DNS (Domain Name System) サーバ、WWW (World Wide Web) サーバ、URL (Uniform Resource Locator) フィルタリングなどの様々な機能を実現するためのソフトウェアを、サーバコンピュータに実装する必要がある。しかも、企業内のネットワークは常時稼働させておく必要がある。そのため、各機能を複数のコンピュータに実装して、一部のコンピュータに障害が発生しても、他のコンピュータによってリカバリできるようなシステム構成となっている。

#### 【0104】

このようなシステム構成を採った場合、各コンピュータに必要なソフトウェアを実装すると共に、そのソフトウェアを利用するためのライセンスを取得する必要がある。このようなライセンス管理を、多数のコンピュータ全てに関して個別に行うのでは、システム管理者にかかる負担が過大となってしまう。

#### 【0105】

そこで、第2の実施の形態では、ネットワークで接続された複数のコンピュータそれぞれで実行されるソフトウェアを一元管理することができるライセンス管理システムを提供する。

#### 【0106】

また、第2の実施の形態では、1つの筐体内に任意の数のコンピュータ機能（プロセッサカートリッジ）を実装できる処理装置の例を用いて説明する。このとき、処理装置の識別情報は筐体に設定される。そこで、第2の実施の形態の説明においては、装置識別情報を筐体IDと呼ぶこととする。

#### 【0107】

図8は、第2の実施の形態に係るライセンス管理システムの概念図である。図8に示すように、第2の実施の形態のシステムの運用には、処理装置提供者24、ライセンス発行局25、ソフトウェア提供者26、及び利用者27が関わって

いる。

#### 【0108】

処理装置提供者 24 は、処理装置 700 を利用者 27 に販売する。処理装置 700 は、筐体、およびその筐体を実装可能なプロセッサモジュールで構成される。処理装置 700 の購入者には、ソフトウェアを実行するために必要なハードウェアキー 50 が渡される。ハードウェアキー 50 は、高い耐タンパ性を有する記憶装置である。たとえば、ハードウェアキーとして、USB (Universal Serial Bus) バスに接続可能なフラッシュメモリを利用することができる。

#### 【0109】

ライセンス発行局 25 は、着脱キー情報をハードウェアキー 50 に格納して、処理装置提供者 24 に提供する。また、ライセンス発行局 25 は、ソフトウェアを暗号化する際の暗号キー（アプリケーション暗号キー）や、ソフトウェアのライセンス情報をソフトウェア提供者 26 に提供する。

#### 【0110】

ソフトウェア提供者 26 は、アプリケーションソフトウェア（以下、単にアプリケーションという）を開発し、利用者に販売する。アプリケーションは、OS 等の基本機能を実現するソフトウェアと共にメモ리카ード 60 に記録され、利用者 27 に渡される。なお、ソフトウェア提供者 26 は、アプリケーションをメモ리카ード 60 に記録する場合、ライセンス発行局 25 から受け取った暗号キーで暗号化したアプリケーションを記録する。

#### 【0111】

利用者 27 は、処理装置提供者 24 から処理装置 700 を購入する。また、利用者 27 は、ソフトウェア提供者 26 からメモ리카ード 60 を購入する。そして、利用者 27 は、ハードウェアキー 50 を処理装置 700 に接続すると共に、メモ리카ード 60 を処理装置 700 内のプロセッサモジュールに差し込む。これにより、処理装置 700 がメモ리카ード 60 に記録されている OS やアプリケーションを実行することが出来る。

#### 【0112】

図 9 は、第 2 の実施の形態におけるライセンス管理機構の概念図である。まず

、処理装置提供者 24 から利用者 27 へ、処理装置 700, 800 が販売される (ステップ S41)。このとき、ライセンス発行局 25 において、処理装置 700 の筐体 ID を含む着脱キー情報が生成される (S42)。生成された着脱キー情報は、ライセンス発行局 25 でハードウェアキー 50 に記録され、処理装置提供者 24 を介して利用者 27 に出荷される (ステップ S43)。

#### 【0113】

また、ライセンス発行局 25 では、アプリケーション暗号キーとアプリケーション複合キーとを発行し、アプリケーション暗号キーをソフトウェア提供者 26 に渡す (ステップ S44)。以下、アプリケーション暗号キーとアプリケーション複合キーとの組を「アプリケーション暗号／復号キー」と表す。ソフトウェア提供者 26 は、そのアプリケーション暗号キーを用いて暗号化前のアプリケーションプログラムを暗号化する (ステップ S45)。暗号化後のアプリケーションプログラムは、メモリカード 60 に格納されて利用者 27 に出荷される (ステップ S46)。

#### 【0114】

さらに、ライセンス発行局 25 では、アプリケーション実行ライセンスを発行する (ステップ S47)。アプリケーション実行ライセンスは、ソフトウェア提供者 26 を介して利用者 27 に提供され、NAS (Network Attached Storage) 900 に格納される (ステップ S48)。NAS 900 は、利用者 27 の社内 LAN (Local Area Network) に接続されたファイル管理用のストレージデバイスである。なお、アプリケーション実行ライセンスは、処理装置 700 からアクセス可能な記録媒体に格納されていればよい。すなわち、NAS 900 以外のコンピュータのストレージデバイスに格納されていてもよい。

#### 【0115】

利用者 27 は、処理装置提供者 24 から購入した処理装置 700, 800 をネットワークに接続し、一方の処理装置 700 にハードウェアキー 50 を装着する。処理装置 700 には、管理用のプロセッサカートリッジ (管理カートリッジ 710) と、アプリケーション実行用の複数のプロセッサカートリッジ (アプリケーションカートリッジ 720) とを有している。管理カートリッジ 710 には、

OS 7 1 1、DHCP (Dynamic Host Configuration Protocol)サーバ 7 1 2 の機能に加え、ライセンス管理マネージャ 7 1 3 が実装されている。ライセンス管理マネージャ 7 1 3 は、NAS 9 0 0 からソフトウェア実行ライセンスを取得し、そのソフトウェア実行ライセンスを、ハードウェアキー 5 0 に記録されている着脱キーを用いて復号する。そして、ライセンス管理マネージャ 7 1 3 は、処理装置 7 0 0 の筐体に設定されている筐体 ID を、ハードウェアキー 5 0 に格納されている筐体 ID との整合性を判断する。筐体 ID が一致すれば、ライセンス管理マネージャ 7 1 3 は他のアプリケーションカートリッジに対して、ソフトウェア実行ライセンスで指定されているライセンス条件に応じたソフトウェアの実行を許可する。

#### 【0 1 1 6】

アプリケーションカートリッジ 7 2 0 には、メモリカード 6 0 が挿入される。アプリケーションカートリッジ 7 2 0 は、処理装置 7 0 0 内で管理カートリッジ 7 1 0 に接続されている。アプリケーションカートリッジ 7 2 0 は、メモリカード 6 0 に記録されている OS やアプリケーション等のプログラムを読み込み、所定の機能を実現する。

#### 【0 1 1 7】

アプリケーションカートリッジ 7 2 0 で実現される機能は、OS 7 2 1、DHCP クライアント 7 2 2、ライセンス管理エージェント 7 2 3、およびアプリケーション 7 2 4 である。ライセンス管理エージェント 7 2 3 は、ライセンス管理マネージャ 7 1 3 からアプリケーション実行許可を受けて、アプリケーションカートリッジ 7 2 0 においてアプリケーション 7 2 4 が実行できるようにする。

#### 【0 1 1 8】

なお、処理装置 8 0 0 のアプリケーションカートリッジ 8 1 0 にメモリカード 7 0 を挿入することで、アプリケーションカートリッジ 8 1 0 内にも、アプリケーションカートリッジ 7 2 0 と同様の機能を構築することが出来る。この際、アプリケーションカートリッジ 8 1 0 は、処理装置 8 0 0 の筐体に設定されている筐体 ID 8 0 1 をライセンス管理マネージャ 7 1 3 に渡すことで、アプリケーションの実行許可を受ける。

**【0119】**

このように、ライセンス管理マネージャ713によって各アプリケーションカートリッジで実行するソフトウェアのライセンスを管理することで、多数のコンピュータで構成されるシステム全体のライセンスを一括管理することができる。しかも、処理装置700、800の筐体IDとハードウェアキー50に設定されている筐体IDとが一致した場合にのみ、その処理装置での実行を可能とするため、装置固有の情報の不正コピーによるソフトウェアの不正使用を防止できる。

**【0120】**

ところで、処理装置700、800には、任意の数のプロセッサカートリッジ（管理カートリッジやアプリケーションカートリッジ）を実装することが出来る。プロセッサカートリッジは、処理装置700、800に実装するだけでLANに接続される。以下、第2の実施の形態に利用される処理装置700、800とプロセッサカートリッジのハードウェア構成について説明する。

**【0121】**

図10は、処理装置のハードウェア構成例を示す図である。処理装置700には、プロセッサカートリッジを実装するための少なくとも1つのスロット（slot #0～slot #n）が設けられている。各スロットには、プロセッサカートリッジを接続するためのコネクタ702a～702mが設けられている。図10の例では、コネクタ702aに管理カートリッジ710が接続され、コネクタ702bとコネクタ702cとにアプリケーションカートリッジ720、730が接続されている。

**【0122】**

また、処理装置700の筐体には、通信インタフェース（I/F）703、識別情報メモリ704、ハブ705、電源ユニット706等が設けられている。なお、ハブ705は、スイッチング機能を有するスイッチングハブであってもよい。また、ハブ705と電源ユニット706が筐体に内蔵されず、外部に接続されていてもよい。

**【0123】**

通信I/F703は、ハードウェアキー50と通信可能な通信インタフェース

である。たとえば、USBインタフェースを利用することが出来る。

識別情報メモリ704は、筐体IDが記録された記録媒体である。たとえば、読み出し専用の半導体メモリが用いられる。識別情報メモリ704は、slot#0のスロットに設けられたコネクタ702aに対してのみ接続されている。したがって、slot#0のスロットに接続された管理カートリッジ710だけが、識別情報メモリ704に記録された筐体IDを直接読み取ることが出来る。なお、識別情報メモリ704が他のスロットに接続されていてもよい。

#### 【0124】

ハブ705は、LAN14に接続されていると共に、各スロットのコネクタ702a～702mに接続されている。これにより、コネクタ702a～702mに接続されたプロセッサカートリッジが、LAN14にも接続される。

#### 【0125】

電源ユニット706は、処理装置700の筐体内に設けられた通信I/F703、識別情報メモリ704、ハブ705に電源を供給すると共に、各コネクタ702a～702mに対して電源を供給している。これにより、コネクタ702a～702mに接続されたプロセッサカートリッジに対して、電源ユニット706から電源が供給される。

#### 【0126】

図11は、プロセッサカートリッジのハードウェア構成例を示す図である。図11では、代表的に管理カートリッジ710の例が示されているが、アプリケーションカートリッジのハードウェア構成も同様である。

#### 【0127】

管理カートリッジ710では、CPU710a、RAM710b、ネットワークインタフェース(I/F)710c、入出力インタフェース(I/F)710d、およびメモ리카ードリーダー・ライター710eがバス710fを介して接続されている。また、管理カートリッジ710にはコネクタ710gが設けられている。このコネクタ710gと処理装置700の筐体に設けられているコネクタ702aとを接続することで、管理カートリッジ710内の回路と処理装置700の筐体内の回路とが電氣的に接続される。

**【0128】**

CPU 710 a は、管理カートリッジ 710 全体を制御する。RAM 710 b は、CPU 710 a が処理を実行するために必要なプログラムやデータが一時的に格納される。ネットワーク I/F 710 c は、ハブ 705 を介して LAN 14 に接続された他の装置（たとえば、他のアプリケーションカートリッジ）と通信する。入出力 I/F 710 d は、通信 I/F 703 や識別情報メモリ 704 に接続され、ハードウェアキー 50 や識別情報メモリ 704 内のデータを読み出し、CPU 710 a 等に転送する。

**【0129】**

なお、図 9 で示した処理装置提供者 24、ライセンス発行局 25、およびソフトウェア提供者 26 で行われる処理にもコンピュータが利用される。そのコンピュータのハードウェア構成は、図 3 に示した第 1 の実施の形態のコンピュータ 100 と同様である。ここで、処理装置提供者 24 で使用されるコンピュータを処理装置管理サーバ、ライセンス発行局 25 で使用されるコンピュータをライセンス発行サーバ、ソフトウェア提供者 26 で使用されるコンピュータをソフトウェア提供サーバと呼ぶこととする。

**【0130】**

図 12 は、各サーバコンピュータの処理機能を示すブロック図である。なお、図 12 では、各装置に含まれる構成要素のみを示し、接続関係（情報の受け渡しを行う関係）を省略している。接続関係については、各構成要素の機能を説明する際に参照する図に示す。図 12 に示すように、処理装置管理サーバ 400 とライセンス発行サーバ 500 とがネットワークを介して接続されている。また、ライセンス発行サーバ 500 とソフトウェア提供サーバ 600 とがネットワークを介して接続されている。なお、処理装置管理サーバ 400、ライセンス発行サーバ 500、ソフトウェア提供サーバ 600 は、それぞれネットワークで接続されていなくてもよい。その場合、各サーバ間の情報の伝達は、可搬型記録媒体等を介して行うことができる。

**【0131】**

処理装置管理サーバ 400 は、処理装置 700、800 の提供元（たとえば、

製造工場、出荷倉庫) またはライセンス発行局 25 に設置され、処理装置の入出庫を管理するコンピュータである。処理装置管理サーバ 400 は、第 2 の実施の形態に係る機能として、着脱キー要求部 410 を有している。

#### 【0132】

着脱キー要求部 410 は、処理装置の筐体に設定されている筐体 ID を含む着脱キー要求を、ネットワークを介してライセンス発行サーバ 500 に対して送信する。なお、着脱キー要求を可搬型記録媒体に格納し、郵送等によりライセンス発行局 25 に渡すこともできる。

#### 【0133】

ライセンス発行サーバ 500 は、アプリケーションソフトウェアのライセンス管理機能を備えたコンピュータである。ライセンス発行サーバ 500 は、着脱キー情報発行部 510、アプリケーション暗号／復号キー発行部 520、ライセンス発行部 530、ライセンス発行費用請求部 540、着脱キー発行記録データベース 550、アプリケーション登録記録データベース 560、ライセンス情報データベース 570、およびライセンス発行記録データベース 580 を有している。

#### 【0134】

着脱キー情報発行部 510 は、処理装置管理サーバ 400 からの着脱キー要求に応答して、着脱キー情報を提供する。具体的には、着脱キー情報発行部 510 は、着脱キー要求を受け取ると、着脱キーの識別情報（着脱キー ID）と、着脱キー固有暗号キーとを生成する。そして、着脱キー ID、着脱キー要求に含まれる筐体 ID、および着脱キー固有暗号キーを含む着脱キー情報を生成する。そして、着脱キー情報発行部 510 は、生成した着脱キー情報を処理装置管理サーバ 400 に送信する。なお、着脱キー情報を可搬型記録媒体に格納し、郵送等により処理装置提供者 24 に渡すこともできる。

#### 【0135】

アプリケーション暗号／復号キー発行部 520 は、ソフトウェア提供サーバ 600 からのアプリケーション暗号キー要求に応答して、アプリケーション暗号キーと、そのアプリケーション暗号キーで暗号化されたデータを復号するためのア

アプリケーション復号キーとを発行する。

【0136】

具体的には、アプリケーションの識別情報（アプリケーションID）を生成して、そのアプリケーションIDに対応するアプリケーション暗号／復号キーを生成する。生成されたアプリケーション暗号／復号キーは、アプリケーション登録記録データベース560に格納される。また、アプリケーション暗号キーは、ソフトウェア提供サーバ600に渡される。

【0137】

ライセンス発行部530は、ソフトウェア提供サーバ600からのライセンス要求に応答して、アプリケーションのライセンスを発行する。具体的には、ライセンス要求を受け取ると、ライセンス発行部530は、利用者27に与えるライセンスの内容を示すアプリケーション実行ライセンスを生成する。次に、ライセンス発行部530は、生成したアプリケーション実行ライセンスを暗号化し、ソフトウェア提供サーバ600に送信する。

【0138】

ライセンス発行費用請求部540は、ライセンスの発行状況（アプリケーション実行している装置数）を監視して、ソフトウェア提供者26からの依頼に基づいて発行したライセンスの発行費用を計算する。ライセンス発行局25では、ライセンス発行費用請求部540で算出されたライセンス発行費用に基づいて、ソフトウェア提供者26に対して費用を請求する。

【0139】

着脱キー発行記録データベース550には、着脱キー情報発行部510によっては発行された着脱キー情報の内容が蓄積されている。

アプリケーション登録記録データベース560には、ライセンスの発行サービスの対象となるアプリケーションに関する情報（アプリケーション情報）が登録されている。たとえば、アプリケーション暗号／復号キーもアプリケーション登録記録データベース560に格納される。

【0140】

ライセンス情報データベース570には、利用者27に対して発行されたライ

センス情報が格納されている。

ライセンス発行記録データベース 580 には、発行されたライセンスの履歴が蓄積されている。ライセンス発行記録データベース 580 を参照すれば、どのアプリケーションに対してどれだけのライセンスを発行したかを集計することができる。

【0141】

ソフトウェア提供サーバ 600 は、暗号キー要求部 610、アプリケーション暗号化部 620、提供ソフトウェア書込部 630、およびソフトウェアライセンス提供部 640 を有している。

【0142】

暗号キー要求部 610 は、ソフトウェア提供者 26 からの操作入力等に応答して、ライセンス発行サーバ 500 に対してアプリケーション暗号キー要求を送信する。たとえば、アプリケーションが完成したときにアプリケーション暗号キー要求が送信される。

【0143】

アプリケーション暗号化部 620 は、ライセンス発行サーバ 500 から送られたアプリケーション暗号キーを用いて、アプリケーションプログラムを暗号化する。

【0144】

提供ソフトウェア書込部 630 は、暗号化されたアプリケーションプログラムと、その他のシステムソフトウェア（OS、ライセンス管理エージェント等）を纏めて、メモリカード 60 に書き込む。

【0145】

ソフトウェアライセンス提供部 640 は、利用者 27 に渡された処理装置 700 からのライセンス要求に応答して、ライセンス発行サーバ 500 に対して、アプリケーション実行ライセンス要求を送信する。ソフトウェアライセンス提供部 640 は、ライセンス発行サーバ 500 からアプリケーション実行ライセンスを受け取ると、そのアプリケーション実行ライセンスを利用者 27 に渡す。たとえば、利用者 27 の管理する NAS 900 にネットワークを介して転送する。

**【0146】**

以下、第2の実施の形態で利用される各種情報のデータ構造例について説明する。

図13は、着脱キーに格納される着脱キー情報のデータ構造例を示す図である。ハードウェアキー50に格納された着脱キー情報52には、着脱キーID52a、筐体ID52b、着脱キー固有暗号キー52cが含まれる。着脱キーID52aは、ハードウェアキー50を一意に識別するための識別情報である。筐体ID52bは、ライセンス発行対象となる処理装置に設定されている識別情報（筐体ID）である。着脱キー固有暗号キー52cは、ハードウェアキー50に対応付けて生成された暗号キーである。

**【0147】**

図14は、着脱キー発行記録データベースのデータ構造例を示す図である。着脱キー発行記録データベース550には、着脱キー情報発行部510で発行された複数の着脱キー情報551, 552, . . . 55nが格納されている。

**【0148】**

図15は、アプリケーション登録記録データベースのデータ構造例を示す図である。アプリケーション登録記録データベースには、複数のアプリケーション情報561, 562, . . . , 56nが登録されている。各アプリケーション情報561, 562, . . . , 56nは、アプリケーションID、アプリケーション暗号／復号キー、および費用請求先の情報を含んでいる。アプリケーションIDは、ライセンス発行サービスの対象となるアプリケーションの識別情報である。アプリケーション暗号／復号キーは、ライセンス発行サービスの対象となるアプリケーションの暗号化および復号に利用される鍵情報である。費用請求先は、アプリケーションに関するライセンス発行サービスを依頼したソフトウェア提供者26を特定するための情報である。費用請求先には、ソフトウェア提供者26の住所、電話番号、顧客整理番号、費用請求方法（たとえば、自動引き落とし金融機関口座情報）などが含まれる。

**【0149】**

図16は、アプリケーション実行ライセンスのデータ構造例を示す図である。

アプリケーション実行ライセンス 80 は、1 以上の筐体 ID 81 a, . . . , 81 i、アプリケーション ID 82、ライセンス数 83、およびアプリケーション復号キー 84 を含んでいる。筐体 ID 81 a, . . . , 81 i は、利用者 27 が連係して動作させる各処理装置に設定された筐体 ID である。アプリケーション ID 82 は、実行を許可するアプリケーションの識別情報である。ライセンス数 83 は、アプリケーションを同時に実行可能なプロセッサカートリッジ数である。アプリケーション復号キー 84 は、アプリケーションを復号するための復号キーである。アプリケーション復号キー 84 は、着脱キー固有暗号キーで暗号化された状態で、アプリケーション実行ライセンス 80 に設定される。

#### 【0150】

図 17 は、ライセンス情報データベースのデータ構造例を示す図である。ライセンス情報データベース 570 には、アプリケーション毎のライセンス情報 571, . . . , 57p が格納されている。各ライセンス情報 571, . . . , 57p は、それぞれアプリケーション ID に対応付けて登録されている。ライセンス情報のデータ構造は、図 16 で示したアプリケーション実行ライセンス 80 の内容と同様である。

#### 【0151】

図 18 は、ライセンス発行記録データベースのデータ構造例を示す図である。ライセンス発行記録データベース 580 には、複数のライセンス発行記録 581, 582, . . . , 58n が格納されている。ライセンス発行記録 581, 582, . . . , 58n には、ライセンス発行日時、アプリケーション ID、およびライセンス数などの情報が含まれている。

#### 【0152】

以上のような構成のライセンス管理システムによって、ソフトウェア提供者 26 によって提供されるアプリケーションを、正当なライセンス所持者である利用者 27 のみ実行できるようにすることができる。第 2 の実施の形態のライセンス管理システムにおける処理は、大別して、ハードウェアキー生成処理、アプリケーション提供処理、ライセンス提供処理、ライセンス発行費用算出処理、およびライセンスに基づくアプリケーション実行処理がある。

**【0153】**

まず、ハードウェアキー生成処理について説明する。

図19は、ハードウェアキー生成処理の概念図である。ハードウェアキーを生成する場合、処理装置管理サーバ400からライセンス発行サーバ500に対して、処理装置700の筐体IDが着脱キー要求と共にネットワークを介して送られる。なお、筐体IDを可搬型記録媒体に格納し、ライセンス発行局25に渡すこともできる。その場合、ライセンス発行局25のオペレータが可搬型記録媒体をライセンス発行サーバ500に挿入し、筐体IDを含む着脱キー要求をライセンス発行サーバ500に入力する。

**【0154】**

具体的には、処理装置管理サーバ400において、着脱キー要求部410が処理装置700の筐体ID701を取得する。たとえば、処理装置の製造工程管理を行っている製造管理装置（図示せず）で筐体IDを取得している場合には、その製造管理装置から筐体IDを取得することができる。また、処理装置管理サーバ400に対する操作入力によって筐体ID701を着脱キー要求部410に通知してもよい。

**【0155】**

筐体ID701を取得した着脱キー要求部410は、ネットワークを介してライセンス発行サーバ500に対して、筐体ID701を含む着脱キー要求を送信する。着脱キー要求は、ライセンス発行サーバ500の着脱キー情報発行部510で受け取られる。なお、筐体ID701を含む着脱キー要求を、ネットワーク以外の情報伝達手段（たとえば、可搬型記録媒体等）を用いてライセンス発行サーバ500に渡すこともできる。

**【0156】**

着脱キー情報発行部510は、処理装置管理サーバ400から受け取った筐体ID701に、着脱キーIDや着脱キー固有暗号キーを関連づけられ、着脱キー情報52を生成する。生成された着脱キー情報52は、メモリライタ501を介してハードウェアキーに書き込まれる。また、着脱キー情報発行部510は、発行した着脱キー情報52を着脱キー発行記録データベース550に格納する。

**【0157】**

着脱キー情報 52 が格納されたハードウェアキー 50 は、処理装置提供者 24 を介して利用者 27 に渡される。なお、ハードウェアキー 50 を、ライセンス発行 25 から利用者 27 に直接渡してもよい。

**【0158】**

図 20 は、着脱キー情報発行部の処理手順を示すフローチャートである。以下、図 20 に示す処理をステップ番号に沿って説明する。以下の処理は、ライセンス発行サーバ 500 に着脱キー要求が渡されたときに実行される処置である。

**【0159】**

〔ステップ S51〕 着脱キー情報発行部 510 は、着脱キー ID を生成する。着脱キー ID としては、ユニークな番号が利用される。

〔ステップ S52〕 着脱キー情報発行部 510 は、着脱キー固有暗号キーを生成する。この着脱キー固有暗号キーは、ライセンス情報の暗号化の際の暗号キーと、ライセンス情報の復号の際の復号キーとを兼ねている。

**【0160】**

〔ステップ S53〕 着脱キー情報発行部 510 は、ハードウェアキー 50 に着脱キー情報（着脱キー ID、筐体 ID、着脱キー固有暗号キー）を書き込む。

〔ステップ S54〕 着脱キー情報発行部 510 は、着脱キー発行記録データベース 550 へ生成した着脱キー情報を着込む。

**【0161】**

以上のようにして、着脱キー情報 52 が記録されたハードウェアキー 50 が生成され、処理装置 700 と共に利用者 27 に提供される。

次に、アプリケーション提供処理について説明する。

**【0162】**

図 21 は、アプリケーション処理の概念図である。ソフトウェア提供者 26 においてアプリケーションプログラム（暗号化前）601 が完成すると、暗号キー要求部 610 からライセンス発行サーバ 500 へ、ネットワークを介してアプリケーション暗号キー要求が出される。なお、アプリケーション暗号キー要求を、ネットワーク以外の情報伝達手段でライセンス発行サーバ 500 に渡してもよい。

。たとえば、ソフトウェア提供者 26 からライセンス発行局 27 へ、電話や電子メール等を用いてアプリケーション暗号キーの発行を依頼し、ライセンス発行局 27 のオペレータがライセンス発行サーバ 500 に対してアプリケーション暗号キー要求を操作入力することもできる。

#### 【0163】

すると、ライセンス発行サーバ 500 のアプリケーション暗号／復号キー発行部 520 がアプリケーション暗号／復号キーを生成し、そのうちのアプリケーション暗号キーのみをソフトウェア提供サーバ 600 に送信する。この際、アプリケーション暗号／復号キー発行部 520 は、生成したアプリケーション暗号／復号キーを、アプリケーション登録記録データベース 560 に格納する。なお、アプリケーション暗号キーは、ネットワーク以外の情報伝達手段によってソフトウェア提供サーバ 600 に渡してもよい。たとえば、アプリケーション暗号キーを可搬型記録媒体に格納し、その可搬型記録媒体を郵送等によりソフトウェア提供者 26 に渡すこともできる。ソフトウェア提供者 26 は、受け取った可搬型記録媒体をソフトウェア提供サーバ 600 に挿入し、ソフトウェア提供サーバ 600 にアプリケーション暗号キーを読み取らせる。

#### 【0164】

ソフトウェア提供サーバ 600 に送られたアプリケーション暗号キーは、アプリケーション暗号化部 620 で受け取られる。アプリケーション暗号化部 620 は、アプリケーション暗号キーを用いて、暗号化前のアプリケーションプログラム 601 を暗号化する。これにより、暗号化後のアプリケーションプログラム 602 が生成される。

#### 【0165】

その後、提供ソフトウェア書込部 630 がアプリケーションプログラム 602 とシステムプログラム 603 とを合わせて、メモリカード 60 に書き込む。システムプログラム 603 には、OS、ライセンス管理エージェント、DHCP クライアントなどの機能を実現するためのプログラム等が含まれる。

#### 【0166】

このようにしてソフトウェアが記録されたメモリカード 60 が利用者 27 に提

供される。

図 22 は、アプリケーション暗号／復号キー発行部の処理手順を示すフローチャートである。以下、図 22 に示す処理をステップ番号に沿って説明する。

【0167】

〔ステップ S61〕 アプリケーション暗号／復号キー発行部 520 は、アプリケーション ID を生成する。アプリケーション ID は、アプリケーション毎にユニークな番号である。

【0168】

〔ステップ S62〕 アプリケーション暗号／復号キー発行部 520 は、アプリケーション暗号／復号キーを生成する。アプリケーション暗号キーとアプリケーション複合キーとは、それぞれアプリケーションの暗号化と復号に使用される。

【0169】

〔ステップ S63〕 アプリケーション暗号／復号キー発行部 520 は、アプリケーション暗号／復号キーをアプリケーション登録記録データベース 560 に書き込む。

【0170】

〔ステップ S64〕 アプリケーション暗号／復号キー発行部 520 は、アプリケーション暗号キーにアプリケーション ID を付与して、ソフトウェア提供サーバ 600 へ送信する。なお、アプリケーション暗号キーを、ネットワーク以外の情報伝達手段によってソフトウェア提供サーバ 600 に渡してもよい。

【0171】

このようにして送信されたアプリケーション暗号キーを用いて、ソフトウェア提供サーバ 600 のアプリケーション暗号化部 620 で、アプリケーションの暗号化が行われる。なお、この例では、アプリケーションが複数のファイルで構成されている。このとき、必ずしも全てのファイルを暗号化する必要はなく、アプリケーションの実行に不可欠なファイル（たとえば、処理機能の起動時に指定する実行形式のファイル）を暗号化すればよい。

【0172】

図 23 は、アプリケーションの暗号化前後の状態を示す図である。暗号化前の

アプリケーションプログラム 601 は、アプリケーション本体 601 a と暗号化情報ファイル 601 b とで構成される。

【0173】

アプリケーション本体 601 a は、複数のファイルで構成される。これらのファイルは、ディレクトリによる階層構造を有している。図 23 の例では、ディレクトリとファイルとの識別番号を、括弧書きで示している。

【0174】

暗号化情報ファイル 601 b は、アプリケーション本体 601 a に含まれるファイルのうち、暗号化対象とするファイルのリストであり、暗号化対象ファイルのファイル名や識別情報が設定されている。図 23 の例では、識別番号が 11、21 のファイルなどが暗号化対象として指定されている。

【0175】

このようなアプリケーションプログラム 601 の暗号化が行われると、暗号化情報ファイル 601 b で暗号化対象として指定されたファイルのみが暗号化される。

【0176】

暗号化後のアプリケーションプログラム 602 は、アプリケーション本体 602 a と暗号化情報ファイル 602 b とで構成されている。アプリケーション本体 602 a に含まれる複数のファイルのうち、暗号化情報ファイル 602 b にリストアップされているファイルのみが暗号化されている。以下、暗号化されたファイルを、暗号化ファイルと呼ぶ。

【0177】

図 24 は、アプリケーション暗号化処理手順を示すフローチャートである。以下、図 24 に示す処理をステップ番号に沿って説明する。

〔ステップ S71〕 アプリケーション暗号化部 620 は、アプリケーションプログラム 602 を複写する。

【0178】

〔ステップ S72〕 アプリケーション暗号化部 620 は、複写されたアプリケーションプログラム 602 の暗号化情報ファイル 602 b から暗号化処理が行わ

れていない暗号化対象ファイルのファイル名を1つ取り出す。

#### 【0179】

〔ステップS73〕アプリケーション暗号化部620は、ステップS72においてファイル名が取り出されたか否かを判断する。すなわち、ファイル名が取り出されていないということは、全ての暗号化対象ファイルの取り出しが終了したことを意味する。全ての暗号化対象ファイルの取り出しが終了していれば、アプリケーション暗号化処理が終了する。暗号化対象ファイルが取り出された場合、処理がステップS74に進められる。

#### 【0180】

〔ステップS74〕アプリケーション暗号化部620は、複製されたアプリケーションプログラム602内の暗号化対象ファイルの暗号化処理を行う。その後、処理がステップS72に進められる。

#### 【0181】

このようにして、アプリケーションプログラム内の予め指定されたファイルのみを暗号化することができる。その結果、暗号化や復号の処理の高速化が図れる。

#### 【0182】

次に、ライセンス提供処理について説明する。

図25は、ライセンス提供処理の概念図である。まず、処理装置700からライセンス取得要求がソフトウェア提供サーバ600に送られる。なお、ライセンス取得要求を、ネットワーク以外の情報伝達手段でソフトウェア提供サーバ600に渡してもよい。

#### 【0183】

ライセンス取得要求がソフトウェア提供サーバ600に渡されると、ソフトウェア提供サーバ600内のソフトウェアライセンス提供部640が、ライセンス発行サーバ500に対して、アプリケーション実行ライセンス要求を送信する。アプリケーション実行ライセンス要求には、ライセンス発行対象となるアプリケーションのアプリケーションID、ライセンス数、動作対象となる処理装置に接続されたハードウェアキーの着脱キーIDなどが含まれる。なお、アプリケーシ

ョン実行ライセンス要求は、ネットワーク以外の情報伝達手段でライセンス発行サーバ500に渡すこともできる。

【0184】

ライセンス発行サーバ500ではライセンス発行部530がアプリケーション実行ライセンス要求を受け取る。すると、ライセンス発行部530は、まずアプリケーション登録記録データベース560を参照し、アプリケーション実行ライセンス要求に含まれるアプリケーションIDに対応するアプリケーション情報を取得する。

【0185】

また、ライセンス発行部530は、着脱キー発行記録データベース550を参照し、動作対象の処理装置の筐体IDに対応する着脱キー情報内のキー固有暗号キーを取得する。次に、ライセンス発行部530は、取得したアプリケーション情報内のアプリケーション復号キーを着脱キー固有暗号キーで暗号化する。その後、暗号化されたアプリケーション復号キーを含めたアプリケーション実行ライセンスを生成し、ライセンス情報データベース570に登録する。そして、ライセンス発行部530は、取得した着脱キー固有暗号キーでアプリケーション実行ライセンスを暗号化する。

【0186】

その後、ライセンス発行部530は、ライセンス発行内容を示す情報をライセンス発行記録データベース580に格納し、暗号化されたアプリケーション実行ライセンスをソフトウェア提供サーバ600に送信する。

【0187】

ソフトウェア提供サーバ600では、ソフトウェアライセンス提供部640がアプリケーション実行ライセンスを受け取り、NAS900（あるいはその他のコンピュータで管理されたストレージデバイス）に転送する。

【0188】

図26は、ライセンス発行部の処理手順を示すフローチャートである。以下、図26に示す処理をステップ番号に沿って説明する。

[ステップS81] ライセンス発行部530は、アプリケーションID、ライ

センス数、動作対象となる処理装置に接続されたハードウェアキーの着脱キー ID などを含むアプリケーション実行ライセンス要求を受け取ると、アプリケーション実行ライセンス 80 を生成する。具体的には、まず、着脱キー発行記録データベース 550 から、アプリケーション実行ライセンス要求で示された着脱キー ID に対応する着脱キー情報を取得する。そして、取得した着脱キー情報から、着脱キー固有暗号キーを抽出する。

#### 【0189】

次に、ライセンス発行部 530 は、アプリケーション実行ライセンス要求で示されたアプリケーション ID に対応するアプリケーション情報をアプリケーション登録記録データベース 560 から抽出する。そして、ライセンス発行部 530 は、抽出したアプリケーション情報内のアプリケーション復号キーを、前に抽出した着脱キー固有暗号キーで暗号化する。さらに、ライセンス発行部 530 は、動作対象となる処理装置の筐体 ID、アプリケーション ID、ライセンス数、着脱キー固有暗号キーで暗号化されたアプリケーション復号キーを含むアプリケーション実行ライセンス 80 を生成する。生成されたアプリケーション実行ライセンス 80 は、ライセンス情報データベース 570 に格納される。

#### 【0190】

[ステップ S82] ライセンス発行部 530 は、生成したアプリケーション実行ライセンスを暗号化する。この例では、着脱キー固有暗号キーで暗号化するものとする。これにより、暗号化後のアプリケーション実行ライセンス 80a が生成される。なお、公開鍵暗号方式の鍵のペア（秘密鍵と公開鍵）を生成し、生成された秘密鍵でアプリケーション実行ライセンスを暗号化してもよい。

#### 【0191】

[ステップ S83] ライセンス発行部 530 は、アプリケーションライセンス発行の記録を、ライセンス発行記録データベース 580 に格納する。アプリケーションライセンスの発行記録としては、ライセンス発行日時、アプリケーション ID、ライセンス数などが含まれる。

#### 【0192】

[ステップ S84] ライセンス発行部 530 は、暗号化後のアプリケーション

実行ライセンス 80a をソフトウェア提供サーバ 600 に送信する。

このようにして、ライセンスが発行される。

#### 【0193】

次に、ライセンス発行費用請求処理について説明する。

図 27 は、ライセンス発行費用請求処理の手順を示すフローチャートである。

以下、図 27 に示す処理をステップ番号に沿って説明する。

#### 【0194】

〔ステップ S91〕ライセンス発行費用請求部 540 は、ライセンス発行記録データベース 580 を参照し、所定の期間内のライセンス発行数をアプリケーション単位で集計する。具体的には、ライセンス発行日時に基づいて、所定の期間（例えば月単位）内のライセンス発行記録を判断し、それらのライセンス発行記録をアプリケーション ID 毎に纏める。そして、纏められたアプリケーション ID 毎のライセンス発行記録内のライセンス数の総計を計算する。

#### 【0195】

〔ステップ S92〕ライセンス発行費用請求部 540 は、ライセンス発行数に応じたライセンス発行費用の請求書を、ソフトウェア提供者 26 に送付する。

次に、処理装置におけるアプリケーション実行処理について説明する。

#### 【0196】

図 28 は、処理装置に構築される処理機能を示すブロック図である。この例では、複数の処理装置 700、800 がネットワークで接続されている。処理装置 700 には、管理カートリッジ 710 とアプリケーションカートリッジ 720 とが接続されている。処理装置 800 には、アプリケーションカートリッジ 810 が接続されている。すなわち、管理カートリッジ 710 は、利用者 27 が管理するシステム内で 1 つだけあればよい。なお、図 28 において、各カートリッジに含まれる機能のうち、OS の機能については省略している。

#### 【0197】

管理カートリッジ 710 は、DHCP サーバ 712、ライセンス管理マネージャ 713、取得済みライセンス情報 714、アプリケーション稼働情報 715 を有している。

**【0198】**

DHCPサーバ712は、利用者27が管理するネットワーク内に接続されたアプリケーションカートリッジに対して、IP(Internet Protocol)アドレスを割り当てる。具体的には、アプリケーションカートリッジ用のIPアドレスを予め用意しておき、アプリケーションカートリッジからのアドレス取得要求に応答して、空いているIPアドレスの情報を送信する。

**【0199】**

ライセンス管理マネージャ713は、アプリケーションカートリッジ720、810で実行されるアプリケーションプログラムのライセンスを管理する。具体的には、アプリケーション実行ライセンスを取得するとその内容を解析し、ライセンス情報を取得済みライセンス情報714に格納する。その際、ハードウェアキー50と筐体ID701とを参照して、アプリケーション実行ライセンスにおいて、処理装置700が動作対象として設定されていることを確認する。

**【0200】**

また、ライセンス管理マネージャ713は、アプリケーションカートリッジからのアプリケーションのライセンス確認要求を受け取ると、取得済みライセンス情報714とアプリケーション稼働情報715とを参照し、実行の可否を判断する。そして、可否の判断結果をアプリケーションカートリッジに返す。

**【0201】**

さらに、ライセンス管理マネージャ713は、アプリケーションの稼働状況を監視し、アプリケーション稼働情報715に設定する。

取得済みライセンス情報714は、取得したアプリケーション実行ライセンスの内容を保持するデータベースである。アプリケーション稼働情報715は、アプリケーションカートリッジ毎のアプリケーションの実行状況が設定されたデータテーブルである。

**【0202】**

なお、取得済みライセンス情報714は、処理装置700からアクセス可能な装置、たとえばNAS900内に設けることができる。図28の例では、管理カートリッジ710内に格納されている場合の例である。

**【0203】**

アプリケーションカートリッジ720は、DHCPクライアント722、ライセンス管理エージェント723、およびアプリケーション724を有している。なお、アプリケーションカートリッジ720が有している機能は、メモリカード60に記録された各種プログラムをアプリケーションカートリッジ720が読み込むことによって構築された機能である。

**【0204】**

DHCPクライアント722は、OSが起動されるとすぐに、DHCPによるIPアドレス取得要求を送信する。そのIPアドレス取得要求に応じてDHCPサーバ712からIPアドレスの情報が返されると、DHCPクライアント722は、そのIPアドレスをアプリケーションカートリッジのIPアドレスに設定する。また、DHCPクライアント722は、IPアドレスの情報の通知に使用されたパケットの送信元アドレスを参照することで、DHCPサーバ712を有する管理カートリッジ710のIPアドレスを認識する。そして、DHCPクライアント722は、管理カートリッジ710のIPアドレスをライセンス管理エージェント723に通知する。これにより、ライセンス管理エージェント723は、ライセンス管理マネージャ713の所在を知ることができる。

**【0205】**

ライセンス管理エージェント723は、メモリカード60に格納されたアプリケーションプログラム602の実行可否をライセンス管理マネージャ713に問い合わせ、実行が許可された場合には、アプリケーションプログラム602の復号処理を行う。ライセンス管理エージェント723がアプリケーションプログラム602を復号し、暗号化前のアプリケーションプログラム601を再現することで、アプリケーション724の機能が動作可能となる。

**【0206】**

アプリケーション724は、メモリカード60に格納されたアプリケーションプログラム602に基づいて実行される処理機能である。

処理装置800に接続されたアプリケーションカートリッジ810は、DHCPクライアント812、ライセンス管理エージェント813、アプリケーション

814を有している。なお、アプリケーションカートリッジ810が有している機能は、メモリカード70に記録された各種プログラムをアプリケーションカートリッジ810が読み込むことによって構築された機能である。

#### 【0207】

ところで、アプリケーションカートリッジ810は、処理装置800のslot#0に接続されている。処理装置800の筐体ID801は、slot#0に接続されたプロセッサカートリッジのみ読み取り可能であるため、アプリケーションカートリッジ810は、筐体ID801を読み取ることが出来る。なお、アプリケーションカートリッジ810が別のスロットに接続されていた場合、slot#0に接続されたプロセッサカートリッジを介して、筐体ID801を取得することができる。また、筐体ID801を格納した識別情報メモリを全てのスロットからアクセスできるように配線しておけば、slot#0以外のスロットに接続されたアプリケーションカートリッジが直接筐体ID801を読み取ることができる。

#### 【0208】

DHCPクライアント812の機能は、アプリケーションカートリッジ720のDHCPクライアント722と同じである。ライセンス管理エージェント813の機能は、アプリケーションカートリッジ720のライセンス管理エージェント723と同じである。アプリケーション814の機能は、アプリケーションカートリッジ720のアプリケーション724と同じである。

#### 【0209】

図29は、取得済みライセンス情報のデータ構造例を示す図である。取得済みライセンス情報714には、複数のアプリケーション実行ライセンス714a, . . . , 714pが格納されている。これらのアプリケーション実行ライセンス714a, . . . , 714pのデータ構造は、図16に示したアプリケーション実行ライセンス80と同じである。なお、取得済みライセンス情報714に格納されているアプリケーション実行ライセンス714a, . . . , 714pは、アプリケーション復号キーを除き、復号された状態（平文）のデータである。なお、改竄防止のために、アプリケーション実行ライセンス714a, . . . , 714pの全体を暗号化して取得済みライセンス情報714に格納しておいてもよい。

。その場合、取得済みライセンス情報 714 からアプリケーション実行ライセンス 714 a, . . . , 714 p を読み出す毎に、アプリケーション実行ライセンス 714 a, . . . , 714 p の復号処理が行われる。

#### 【0210】

図 30 は、アプリケーション稼働情報のデータ構造例を示す図である。アプリケーション稼働情報 715 には、処理装置毎のアプリケーション稼働テーブル 715 a, . . . , 715 m が設けられている。アプリケーション稼働テーブル 715 a, . . . , 715 m は、対応する処理装置のどのスロットのアプリケーションカートリッジでどのアプリケーションが実行されているのかを示している。

#### 【0211】

具体的には、アプリケーション稼働テーブル 715 a, . . . , 715 m は、格子状のテーブルであり、縦軸に沿ってアプリケーション ID が振られ、横軸に沿ってスロット番号が振られている。アプリケーション ID とスロット番号とで特定されるセルに 1 が設定されていれば、対応するスロット番号に接続されたアプリケーションカートリッジで、アプリケーション ID で示されたアプリケーションが実行されていることを表している。

#### 【0212】

以上のような構成の処理装置 700, 800 によって、正当なライセンスを受けたアプリケーションを実行することができる。

まず、ライセンス管理エージェント 723 におけるアプリケーション起動について説明する。

#### 【0213】

図 31 は、アプリケーション起動処理の手順を示すフローチャートである。この処理は、アプリケーションの起動要求が出されたときに開始される。アプリケーションの起動要求は、OS の起動時に自動的に OS からさせることができる。また、利用者 27 の操作入力によってアプリケーションの起動要求が出されるようにしてもよい。以下、図 31 に示す処理をステップ番号に沿って説明する。

#### 【0214】

[ステップ S101] ライセンス管理エージェント 723 は、アプリケーショ

ン実行可否の判定依頼（ライセンス確認要求）をライセンス管理マネージャ 713 に送信する。ライセンス確認要求には、アプリケーション ID と筐体 ID とが含まれる。なお、処理装置の slot#0 に接続されたアプリケーションカートリッジであれば、直接筐体 ID を読み取り、ライセンス確認要求に付加することが出来る。それ以外のスロットに接続されたアプリケーションカートリッジは、slot#0 に接続されたプロセッサカートリッジ（管理カートリッジもしくはアプリケーションカートリッジ）に問い合わせることで、筐体 ID を取得することが出来る。なお、筐体 ID が記録された識別情報メモリを全てのスロットに接続しておけば、全てのアプリケーションカートリッジが直接筐体 ID を読み取ることができる。

#### 【0215】

〔ステップ S102〕 ライセンス管理エージェント 723 は、ライセンス管理マネージャ 713 からのアプリケーション実行可否判定結果を待つ。アプリケーション実行可否結果を受け取ったら、処理がステップ S103 に進められる。なお、アプリケーションの実行が許可される場合には、アプリケーション実行可否結果にアプリケーション復号キーが含まれる。

#### 【0216】

〔ステップ S103〕 ライセンス管理エージェント 723 は、ライセンス管理マネージャ 713 からの応答内容を判定する。アプリケーションの実行が許可された場合には、処理がステップ S106 に進められる。アプリケーションの実行が不許可の場合には、処理がステップ S104 に進められる。

#### 【0217】

〔ステップ S104〕 ライセンス管理エージェント 723 は、アプリケーションの起動要求を出したプロセスに対して、アプリケーション実行不可のメッセージを通知する。

#### 【0218】

〔ステップ S105〕 ライセンス管理エージェント 723 は、一定時間待機する。その後、処理がステップ S101 に進められる。

〔ステップ S106〕 ライセンス管理エージェント 723 は、アプリケーショ

ンの実行が許可されると、アプリケーションプログラムの復号処理を行う。この処理の詳細は後述する。

#### 【0219】

〔ステップS107〕ライセンス管理エージェント723は、復号されたアプリケーションプログラムの実行ファイルの実行要求を出力し、アプリケーションを起動する。

#### 【0220】

図32は、アプリケーションプログラム復号処理の手順を示すフローチャートである。以下、図32に示す処理をステップ番号に沿って説明する。

〔ステップS111〕ライセンス管理エージェント723は、暗号化情報ファイル602bから未処理の暗号化対象ファイルのファイル名を取り出す。

#### 【0221】

〔ステップS112〕ライセンス管理エージェント723は、全ての暗号化対象ファイル名の取り出しが終了したか否かを判断する。すなわち、ステップS111において未処理の暗号化対象ファイルのファイル名が見つからなかった場合には、全ての暗号化対象ファイル名の取り出しが終了したものと判断し、処理を終了する。暗号化対象ファイルのファイル名が取り出された場合には、処理がステップS113に進められる。

#### 【0222】

〔ステップS113〕ライセンス管理エージェント723は、取り出したファイル名に対応するファイルをアプリケーション本体602aから取り出し、復号する。復号する際の復号キーは、実行可否判定結果と共にライセンス管理マネージャ713から渡されたアプリケーション復号キーである。

#### 【0223】

ファイルの復号完了後、処理がステップS111に進められる。

このようにして、ライセンス管理エージェントによって復号されたアプリケーションプログラムにより、アプリケーションが起動される。この際、ライセンス管理マネージャ713は、アプリケーション実行の許可を出したことで、アプリケーションカートリッジ720によってアプリケーション724が実行されてい

ることを認識できる。

#### 【0224】

ここで、アプリケーションの実行が終了した場合には、その旨をライセンス管理マネージャ713に通知する必要がある。このようなアプリケーションの動作状態の通知処理は、ライセンス管理エージェント723が行う。

#### 【0225】

図33は、アプリケーション終了時の処理手順を示すフローチャートである。以下、図33に示す処理をステップ番号に沿って説明する。

[ステップS121] ライセンス管理エージェント723は、アプリケーションが終了したか否かを判断する。終了した場合には、処理がステップS122に進められる。終了していない場合には、ステップS121の処理が繰り返される。これにより、ライセンス管理エージェント723によって、アプリケーションの動作状態が監視される。

#### 【0226】

[ステップS122] ライセンス管理エージェント723は、アプリケーションが終了したことをライセンス管理マネージャに通知する。

このようにして、アプリケーションが終了すると、その旨がライセンス管理マネージャ713に通知される。

#### 【0227】

なお、第2の実施の形態では、定期的にアプリケーションの実行継続の可否が判定され、実行継続が許可された場合にのみ続けてアプリケーションを実行することが出来る。

#### 【0228】

図34は、アプリケーション実行継続監視処理の手順を示すフローチャートである。以下、図34に示す処理をステップ番号に沿って説明する。

[ステップS131] ライセンス管理エージェント723は、アプリケーション実行継続の可否判定依頼をライセンス管理マネージャ713に送信する。アプリケーション実行継続の可否判定依頼には、アプリケーションIDと筐体IDとが含まれる。

**【0229】**

〔ステップS132〕ライセンス管理エージェント723は、アプリケーション実行継続可否の判定結果を待つ。アプリケーション実行継続可否判定結果を受け取った処理がステップS133に進められる。また、ライセンス管理マネージャ713と通信が出来ないと判断した場合にも処理がステップS133に進められる。

**【0230】**

〔ステップS133〕ライセンス管理エージェント723は、アプリケーションの実行継続の可否を判断する。実行継続可能と判断するのは、継続可能というアプリケーション実行継続可否判定結果を受け取った場合である。継続不可能というアプリケーション実行継続可否判定結果を受け取った場合、およびライセンス管理マネージャ713と通信が出来なかった場合には、実行継続不可と判断する。実行継続可能な場合には、処理がステップS136に進められる。実行継続不可の場合には、処理がステップS134に進められる。

**【0231】**

〔ステップS134〕ライセンス管理エージェント723は、アプリケーションを実行しているプロセスに対して、アプリケーション継続不可のメッセージを通知する。

**【0232】**

〔ステップS135〕ライセンス管理エージェント723は、アプリケーションを実行しているプロセスを強制停止する。その後、処理がステップS136に進められる。

**【0233】**

〔ステップS136〕ライセンス管理エージェント723は、一定時間待ち合わせを行う。所定の待ち合わせ時間が経過したら処理がステップS131に進められる。

**【0234】**

このような処理がアプリケーション終了処理が行われるまで繰り返し実行される。

次に、ライセンス管理マネージャ 713 で実行される処理について図 35 ～図 38 を参照して具体的に説明する

図 35 は、ライセンス管理マネージャの処理手順を示す第 1 のフローチャートである。以下、図 35 に示す処理をステップ番号に沿って説明する。

#### 【0235】

〔ステップ S201〕 ライセンス管理マネージャ 713 は、ライセンス管理エージェントからの依頼の待ち合わせを行う。ライセンス管理エージェントから何らかの依頼を受信したら処理がステップ S202 に進められる。なお、ライセンス管理エージェントから何らかの依頼には、アプリケーション ID と筐体 ID とが含まれる。

#### 【0236】

〔ステップ S202〕 ライセンス管理マネージャ 713 は、ライセンス管理エージェントから受け取った依頼が、アプリケーション実行可否の判定依頼であるか否かを判断する。アプリケーション実行可否の判定依頼であれば、処理がステップ S203 に進められる。アプリケーション実行可否の判定依頼でなければ、処理が図 37 のステップ S221 に進められる。

#### 【0237】

〔ステップ S203〕 ライセンス管理マネージャ 713 は、ハードウェアキー 50 に格納されている着脱キー情報を参照する。

〔ステップ S204〕 ライセンス管理マネージャ 713 は、アプリケーション実行ライセンスを暗号化したときのアルゴリズムに応じた復号アルゴリズムで、アプリケーション実行ライセンスを復号する。具体的には、ライセンス管理マネージャ 713 は、アプリケーション実行可否の判定依頼で示されるアプリケーション ID に対応するアプリケーション実行ライセンスを取得済みライセンス情報 714 から取得する。そして、ハードウェアキー 50 に格納されている着脱キー情報内の着脱キー固有暗号キーを用いて、アプリケーション実行ライセンスを復号する。

#### 【0238】

なお、公開鍵暗号化方式を用いて公開鍵と秘密鍵を生成し、その秘密鍵によっ

てアプリケーション実行ライセンスが暗号化されている場合には、秘密鍵と同時に生成された公開鍵を用いて復号する。

#### 【0 2 3 9】

〔ステップ S 2 0 5〕 ライセンス管理マネージャ 7 1 3 は、着脱キー情報の筐体 I D が、処理装置 7 0 0 固有の筐体 I D 7 0 1 と一致するか否かを判断する。筐体 I D が一致すれば処理がステップ S 2 0 6 に進められる。筐体 I D が一致しなければ、処理が図 3 6 のステップ S 2 1 6 に進められる。

#### 【0 2 4 0】

〔ステップ S 2 0 6〕 ライセンス管理マネージャ 7 1 3 は、筐体 I D が、ステップ S 2 0 4 で復号されたアプリケーション実行ライセンスにおいて、動作対象の筐体 I D として設定されているか否かを判断する。動作対象の筐体 I D として設定されていれば、処理が図 3 6 のステップ S 2 1 1 に進められる。動作対象の筐体 I D として設定されていなければ、処理が図 3 6 のステップ S 2 1 6 に進められる。

#### 【0 2 4 1】

図 3 6 は、ライセンス管理マネージャの処理手順を示す第 2 のフローチャートである。以下、図 3 6 に示す処理をステップ番号に沿って説明する。

〔ステップ S 2 1 1〕 ライセンス管理マネージャ 7 1 3 は、アプリケーション稼働情報 7 1 5 の更新をロックする。

#### 【0 2 4 2】

〔ステップ S 2 1 2〕 ライセンス管理マネージャ 7 1 3 は、取得済みライセンス情報 7 1 4 とアプリケーション稼働情報 7 1 5 とを参照し、アプリケーション実行の可否を判定する。具体的には、ライセンス管理マネージャ 7 1 3 は、アプリケーション稼働情報 7 1 5 を参照し、判定対象のアプリケーションを実行中のアプリケーションカートリッジ数（稼働数）を数える。そして、ライセンス管理マネージャ 7 1 3 は、稼働数と、ステップ S 2 0 4 で復号されたアプリケーション実行ライセンス内のライセンス数とを比較する。ライセンス数の方が大きければ、アプリケーション実行可能と判断する。そうでなければ、アプリケーション実行不可と判断する。

**【0243】**

アプリケーション実行可能と判断した場合、処理がステップS213に進められる。アプリケーション実行不可と判断した場合、処理がステップS214に進められる。

**【0244】**

〔ステップS213〕 ライセンス管理マネージャ713は、稼働数の値に1を加算する。

〔ステップS214〕 ライセンス管理マネージャ713は、アプリケーション稼働情報715の更新ロックを解除する。

**【0245】**

〔ステップS215〕 ライセンス管理マネージャ713は、アプリケーション実行ライセンスに含まれるアプリケーション復号キーを、着脱キー固有暗号キーで復号する。

**【0246】**

〔ステップS216〕 ライセンス管理マネージャ713は、アプリケーション実行可否の判定結果を、判定を依頼したライセンス管理エージェントに通知する。判定結果には、ステップS215で復号されたアプリケーション復号キーが含まれる。その後、処理が図35のステップS201に進められる。

**【0247】**

図37は、ライセンス管理マネージャの処理手順を示す第3のフローチャートである。以下、図37に示す処理をステップ番号に沿って説明する。

〔ステップS221〕 ライセンス管理マネージャ713は、受け取った依頼が、アプリケーション実行継続の可否判定依頼であるか否かを判断する。アプリケーション実行継続の可否判定依頼には、アプリケーションIDや筐体IDが含まれる。実行継続可否の判定依頼であれば、処理がステップS222に進められる。実行継続可否の判定依頼でなければ処理が図38のステップS231に進められる。

**【0248】**

〔ステップS222〕 ライセンス管理マネージャ713は、ハードウェアキー

50に格納されている着脱キー情報を参照する。

【ステップS223】ライセンス管理マネージャ713は、アプリケーション実行ライセンスを暗号化したときのアルゴリズムに応じた復号アルゴリズムで、アプリケーション実行ライセンスを復号する。具体的には、ライセンス管理マネージャ713は、アプリケーション実行継続可否の判定依頼で示されるアプリケーションIDに対応するアプリケーション実行ライセンスを取得済みライセンス情報714から取得する。そして、ハードウェアキー50に格納されている着脱キー情報内の着脱キー固有暗号キーを用いて、アプリケーション実行ライセンスを復号する。

#### 【0249】

なお、公開鍵暗号化方式を用いて公開鍵と秘密鍵を生成し、その秘密鍵によってアプリケーション実行ライセンスが暗号化されている場合には、秘密鍵と同時に生成された公開鍵を用いて復号する。

#### 【0250】

【ステップS224】ライセンス管理マネージャ713は、筐体IDが、ステップS223で復号されたアプリケーション実行ライセンスにおいて動作対象の筐体IDとして設定されているか否かを判断する。動作対象の筐体IDとして設定されていれば、処理がステップS225に進められる。動作対象の筐体IDとして設定されていなければ、処理がステップS227に進められる。

#### 【0251】

【ステップS225】ライセンス管理マネージャ713は、着脱キー情報の筐体IDが、処理装置700固有の筐体ID701と一致するか否かを判断する。筐体IDが一致すれば処理がステップS226に進められる。筐体IDが一致しなければ、処理がステップS227に進められる。

#### 【0252】

【ステップS226】ライセンス管理マネージャ713は、アプリケーションの実行を継続可と判定する。その後、処理がステップS228に進められる。

【ステップS227】ライセンス管理マネージャ713は、アプリケーションの実行を継続不可と判定する。

**【0253】**

〔ステップS228〕ライセンス管理マネージャ713は、アプリケーション実行継続可否の判定結果を、判定を依頼したアプリケーション管理エージェントに通知する。その後、処理がステップS201に進められる。

**【0254】**

図38は、ライセンス管理マネージャの処理手順を示す第4のフローチャートである。以下、図38に示す処理をステップ番号に沿って説明する。

〔ステップS231〕ライセンス管理マネージャ713は、ライセンス管理エージェントからの依頼がアプリケーション終了の通知か否かを判断する。アプリケーション終了の通知の場合には、処理がステップS232に進められる。そうでない場合には、処理が図35のステップS201に進められる。

**【0255】**

〔ステップS232〕ライセンス管理マネージャ713は、アプリケーション稼働情報715の更新をロックする。

〔ステップS233〕ライセンス管理マネージャ713は、終了したアプリケーションの稼働数を1だけ減算する。

**【0256】**

〔ステップS234〕ライセンス管理マネージャ713は、アプリケーション稼働情報の更新ロックを解除する。その後、処理が図35のステップS201に進められる。

**【0257】**

以上のようにして、アプリケーションの不正使用を確実に防止したライセンス管理が可能となる。すなわち、装置識別情報（筐体ID）を埋め込んだハードウェアキーを提供し、ハードウェアキーに設定された装置識別情報と、アプリケーションを実行する処理装置の装置識別情報とが一致しなければアプリケーションが実行できない。その結果、処理装置の偽装等の不正行為を防止することができる。

**【0258】**

また、ハードウェアキーをライセンス発行局で発行するため、ライセンス管理

を厳密に行うことができる。ただし、利便性等を優先し、ソフトウェア提供者がハードウェアキーを発行するようにしてもよい。

#### 【0 2 5 9】

しかも、各アプリケーションカートリッジが処理装置の筐体に装着されると、自動的にライセンス確認依頼が管理カートリッジに出され、ライセンス数で定められた数以内のアプリケーションカートリッジに対してのみアプリケーションの実行が許可される。したがって、アプリケーションカートリッジに対して個別にライセンス情報を設定する必要がなくなり、利用者 2 7 のシステム管理が容易となる。

#### 【0 2 6 0】

また、管理カートリッジでは、現在アプリケーションを実行しているアプリケーションカートリッジ数を常に把握している。そして、メンテナンスのためにアプリケーションを実行しているアプリケーションカートリッジを抜き取った場合、そのアプリケーションを実行可能な他のアプリケーションカートリッジに対して、自動的に実行の許可が出される。そのため、処理装置のメンテナンス時におけるシステム全体の処理効率の低下を防ぐことが出来る。

#### 【0 2 6 1】

なお、上記の第 2 の実施の形態では、ライセンス発行サーバ 5 0 0 とソフトウェア提供サーバ 6 0 0 との機能を分けているが、1 つのサーバ（たとえば、ソフトウェア提供サーバ）でハードウェアキーへの着脱キー情報の書き込み、ソフトウェアの提供、ライセンスの発行を行ってもよい。

#### 【0 2 6 2】

なお、上記の第 1、第 2 の実施の形態では、装置識別情報（筐体 I D）をメモリに記録するものとしているが、このメモリは装置に固定されたデータ保持可能な回路であればよい。たとえば、C P U 内部に設定されている C P U の識別情報を装置識別情報として使用することもできる。

#### 【0 2 6 3】

また、上記の第 1 の実施の形態では、ソフトウェア暗号キーとソフトウェア復号キーとの 2 つの鍵情報を生成しているが、1 つの鍵情報を、ソフトウェア暗号

キーとソフトウェア復号キーとの両方に使用してもよい。同様に、上記の第2の実施の形態では、アプリケーション暗号キーとアプリケーション復号キーとの2つの鍵情報を生成しているが、1つの鍵情報を、アプリケーション暗号キーとアプリケーション復号キーとの両方に使用してもよい。

#### 【0264】

なお、上記の処理機能は、コンピュータによって実現することができる。その場合、処理装置管理サーバ、ライセンス発行サーバ、ソフトウェア提供サーバ、および処理装置内の各プロセッサカートリッジが有すべき機能の処理内容を記述したプログラムが提供される。そのプログラムをコンピュータで実行することにより、上記処理機能がコンピュータ上で実現される。処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリなどがある。磁気記録装置には、ハードディスク装置（HDD）、フレキシブルディスク（FD）、磁気テープなどがある。光ディスクには、DVD(Digital Versatile Disc)、DVD-RAM(Random Access Memory)、CD-ROM(Compact Disc Read Only Memory)、CD-R(Recordable)/RW(ReWritable)などがある。光磁気記録媒体には、MO(Magneto-Optical disc)などがある。

#### 【0265】

プログラムを流通させる場合には、たとえば、そのプログラムが記録されたDVD、CD-ROMなどの可搬型記録媒体が販売される。また、プログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することもできる。

#### 【0266】

プログラムを実行するコンピュータは、たとえば、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、自己の記憶装置に格納する。そして、コンピュータは、自己の記憶装置からプログラムを読み取り、プログラムに従った処理を実行する。なお、コンピュータは、可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行

することもできる。また、コンピュータは、サーバコンピュータからプログラムが転送される毎に、逐次、受け取ったプログラムに従った処理を実行することもできる。

#### 【0 2 6 7】

(付記1) ソフトウェアの実行ライセンスを発行するライセンス発行サーバにおいて、

前記ソフトウェアの暗号化のための暗号キー生成要求に応じて、ソフトウェア暗号キーと、前記ソフトウェア暗号キーで暗号化された前記ソフトウェアを復号するためのソフトウェア復号キーとを生成するソフトウェア暗号キー生成手段と、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含むライセンス発行要求に応じて、前記装置識別情報で前記ソフトウェア復号キーを暗号化し、暗号化された前記ソフトウェア復号キーを含むソフトウェアライセンスを出力するライセンス発行手段と、

を有することを特徴とするライセンス発行サーバ。

#### 【0 2 6 8】

(付記2) 前記ソフトウェア暗号キー生成手段は、前記暗号キー生成要求が、ネットワークを介して接続された他のコンピュータから送られた場合、生成した前記ソフトウェア暗号キーを前記他のコンピュータへ送信することを特徴とする付記1記載のライセンス発行サーバ。

#### 【0 2 6 9】

(付記3) 前記ライセンス発行手段は、前記ライセンス発行要求が、ネットワークを介して接続された他のコンピュータから送られた場合、生成した前記ソフトウェアライセンスを前記他のコンピュータへ送信することを特徴とする付記1記載のライセンス発行サーバ。

#### 【0 2 7 0】

(付記4) ライセンスによって実行を制限すべきソフトウェアを提供するソフトウェア提供サーバにおいて、

前記ソフトウェアの暗号化のための暗号キー生成要求に応じて、ソフトウェア

暗号キーと、前記ソフトウェア暗号キーで暗号化された前記ソフトウェアを復号するためのソフトウェア復号キーとを生成するソフトウェア暗号キー生成手段と、

前記ソフトウェア暗号キー生成手段で生成された前記ソフトウェア暗号キーを用いて、前記ソフトウェアを暗号化するソフトウェア暗号化手段と、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含むソフトウェア要求が前記処理装置から入力されると、前記ソフトウェア暗号化手段で暗号化された前記ソフトウェアを前記処理装置へ送信するソフトウェア提供手段と、

前記ソフトウェア要求が前記処理装置から入力されると、前記装置識別情報で前記ソフトウェア復号キーを暗号化し、暗号化された前記ソフトウェア復号キーを含むソフトウェアライセンスを前記処理装置へ送信するライセンス発行手段と、

を有することを特徴とするソフトウェア提供サーバ。

#### 【0271】

(付記5) ライセンスによって実行が制限されたソフトウェアを実行する処理装置において、

装置識別情報が固定的に記録された記録媒体と、

暗号化された状態のソフトウェア復号キーを受け取ると、前記記録媒体に記録された前記装置識別情報を復号キーとして前記ソフトウェア復号キーを復号する復号キー復号手段と、

前記ソフトウェア提供サーバから暗号化された状態の前記ソフトウェアを受け取ると、前記復号キー復号手段で復号された前記ソフトウェア復号キーを復号キーとして前記ソフトウェアを復号するソフトウェア復号手段と、

を有することを特徴とする処理装置。

#### 【0272】

(付記6) ソフトウェアの実行ライセンスを発行するライセンス発行サーバにおいて、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録

された装置識別情報を含む着脱キー情報生成要求に応答して、前記装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報を生成し、生成した前記着脱キー情報を、前記処理装置に着脱可能なハードウェアキーに記録する着脱キー情報発行手段と、

前記ソフトウェアのライセンス発行要求に応じて、暗号化された状態で提供される前記ソフトウェアを復号するためのソフトウェア復号キーを前記着脱キー固有暗号キーで暗号化して、暗号化された前記ソフトウェア復号キーを含むライセンス情報を出力するライセンス発行手段と、

を有することを特徴とするライセンス発行サーバ。

#### 【0 2 7 3】

(付記 7) 前記ライセンス発行手段は、前記ソフトウェアを同時に実行可能な装置数を示すライセンス数を、前記ライセンス情報に含めることを特徴とする付記 6 記載のライセンス発行サーバ。

#### 【0 2 7 4】

(付記 8) 前記ハードウェアキーは、耐タンパ性を有していることを特徴とする付記 6 記載のライセンス発行サーバ。

(付記 9) 前記ライセンス発行手段は、前記ライセンス情報を暗号化して出力することを特徴とする付記 6 記載のライセンス発行サーバ。

#### 【0 2 7 5】

(付記 1 0) 前記ライセンス発行手段は、前記着脱キー固有暗号キーで前記ライセンス情報を暗号化することを特徴とする付記 9 記載のライセンス発行サーバ。

#### 【0 2 7 6】

(付記 1 1) 前記ライセンス発行手段により出力された前記ライセンス情報の履歴を蓄積し、蓄積された前記ライセンス情報に基づいて、前記ソフトウェアの提供者に対して請求するライセンス発行手数料を算出するライセンス発行費用算出手段をさらに有することを特徴とする付記 6 記載のライセンス発行サーバ。

#### 【0 2 7 7】

(付記 1 2) ライセンスによって実行を制限すべきソフトウェアを提供する

ソフトウェア提供サーバにおいて、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含む着脱キー情報生成要求に応答して、前記装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報を生成し、生成した前記着脱キー情報を、前記処理装置に着脱可能なハードウェアキーに記録する着脱キー情報発行手段と、

前記ソフトウェアの暗号化と復号とのためのソフトウェア暗号キーと、前記ソフトウェア暗号キーで暗号化されたデータを復号するためのソフトウェア復号キーとを生成するソフトウェア暗号キー生成手段と、

前記ソフトウェア暗号キー生成手段で生成された前記ソフトウェア暗号キーを用いて、前記ソフトウェアを暗号化するソフトウェア暗号化手段と、

ソフトウェア要求が前記処理装置から入力されると、前記ソフトウェア暗号化手段で暗号化された前記ソフトウェアを前記処理装置へ送信するソフトウェア提供手段と、

前記ソフトウェアのライセンス発行要求に応じて、前記ソフトウェア復号キーを前記着脱キー固有暗号キーで暗号化して、暗号化された前記ソフトウェア復号キーを含むライセンス情報を出力するライセンス発行手段と、

を有することを特徴とするソフトウェア提供サーバ。

#### 【0278】

(付記13) ライセンスによって実行が制限されたソフトウェアを実行する処理装置において、

装置識別情報が固定的に記録された記録媒体と、

動作許可対象装置を特定する許可対象装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報が格納されたハードウェアキーが装着されたとき、前記ハードウェアキーから前記着脱キー情報を読み取るハードウェアキー接続手段と、

暗号化された状態の前記ソフトウェアを復号するためのソフトウェア復号キーが暗号化された状態で含まれたライセンス情報が入力されると、前記ソフトウェア復号キーを前記着脱キー固有暗号キーで復号するソフトウェア復号手段と

、

前記ハードウェアキー接続手段に接続された前記ハードウェアキーに含まれる前記許可対象識別情報と前記記録媒体に記録された装置識別情報との同一性を判定する識別情報判定手段と、

前記識別情報判定手段により、同一であると判定された場合には、前記ソフトウェアキー復号手段で復号された前記ソフトウェア復号キーで、暗号化された状態の前記ソフトウェアを復号するソフトウェア復号手段と、

を有することを特徴とする処理装置。

#### 【0 2 7 9】

(付記 1 4) ライセンスによって実行が制限されたソフトウェアの実行状況を管理するソフトウェア実行管理装置において、

装置識別情報が固定的に記録された記録媒体と、

動作許可対象装置を特定する許可対象装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報が格納されたハードウェアキーが装着されたとき、前記ハードウェアキーから前記着脱キー情報を読み取るハードウェアキー接続手段と、

暗号化された状態の前記ソフトウェアを復号するための暗号化されたソフトウェア復号キーと同時実行可能なコンピュータ数とが含まれたライセンス情報が入力されると、前記ソフトウェア復号キーを前記着脱キー固有暗号キーで復号するソフトウェアキー復号手段と、

ネットワークを介して接続されたコンピュータのうち前記ソフトウェアを実行している実行コンピュータ数を監視し、前記同時実行可能なコンピュータ数以下の数の前記コンピュータに対して、前記ソフトウェアキー復号手段で復号された前記ソフトウェア復号キーを渡す復号キー管理手段と、

を有することを特徴とするソフトウェア実行管理装置。

#### 【0 2 8 0】

(付記 1 5) ソフトウェアの実行ライセンスを発行するためのライセンス発行方法において、

前記ソフトウェアの暗号化のための暗号キー生成要求に応じて、ソフトウェア暗号キーと、前記ソフトウェア暗号キーで暗号化された前記ソフトウェアを復号するためのソフトウェア復号キーとを生成し、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含むライセンス発行要求に応じて、前記装置識別情報で前記ソフトウェア復号キーを暗号化し、暗号化された前記ソフトウェア復号キーを含むソフトウェアライセンスを出力する、

ことを特徴とするライセンス発行方法。

#### 【0281】

(付記16) ソフトウェアの実行ライセンスを発行するためのライセンス発行方法において、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含む着脱キー情報生成要求に応答して、前記装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報を生成し、生成した前記着脱キー情報を、前記処理装置に着脱可能なハードウェアキーに記録し、

前記ソフトウェアのライセンス発行要求に応じて、暗号化された状態で提供される前記ソフトウェアを復号するためのソフトウェア復号キーを前記着脱キー固有暗号キーで暗号化して、暗号化された前記ソフトウェア復号キーを含むライセンス情報を出力する、

ことを特徴とするライセンス発行方法。

#### 【0282】

(付記17) ソフトウェアの実行ライセンスを発行するためのライセンス発行プログラムにおいて、

コンピュータに、

前記ソフトウェアの暗号化のための暗号キー生成要求に応じて、ソフトウェア暗号キーと、前記ソフトウェア暗号キーで暗号化された前記ソフトウェアを復号するためのソフトウェア復号キーとを生成し、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含むライセンス発行要求に応じて、前記装置識別情報で前記ソフトウェア復号キーを暗号化し、暗号化された前記ソフトウェア復号キーを含むソフトウェアライセンスを出力する、

処理を実行させることを特徴とするライセンス発行プログラム。

**【0283】**

(付記18) ソフトウェアの実行ライセンスを発行するためのライセンス発行プログラムにおいて、

コンピュータに、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含む着脱キー情報生成要求に応答して、前記装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報を生成し、生成した前記着脱キー情報を、前記処理装置に着脱可能なハードウェアキーに記録し、

前記ソフトウェアのライセンス発行要求に応じて、暗号化された状態で提供される前記ソフトウェアを復号するためのソフトウェア復号キーを前記着脱キー固有暗号キーで暗号化して、暗号化された前記ソフトウェア復号キーを含むライセンス情報を出力する、

処理を実行させることを特徴とするライセンス発行プログラム。

**【0284】**

(付記19) ソフトウェアの実行ライセンスを発行するためのライセンス発行プログラムを記録したコンピュータ読み取り可能な記録媒体において、

前記コンピュータに、

前記ソフトウェアの暗号化のための暗号キー生成要求に応じて、ソフトウェア暗号キーと、前記ソフトウェア暗号キーで暗号化された前記ソフトウェアを復号するためのソフトウェア復号キーとを生成し、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含むライセンス発行要求に応じて、前記装置識別情報で前記ソフトウェア復号キーを暗号化し、暗号化された前記ソフトウェア復号キーを含むソフトウェアライセンスを出力する、

処理を実行させることを特徴とするライセンス発行プログラムを記録したコンピュータ読み取り可能な記録媒体。

**【0285】**

(付記20) ソフトウェアの実行ライセンスを発行するためのライセンス発行プログラムを記録したコンピュータ読み取り可能な記録媒体において、

前記コンピュータに、

前記ソフトウェアの動作許可対象である処理装置内の記録媒体に固定的に記録された装置識別情報を含む着脱キー情報生成要求に応答して、前記装置識別情報と着脱キー固有暗号キーとを含む着脱キー情報を生成し、生成した前記着脱キー情報を、前記処理装置に着脱可能なハードウェアキーに記録し、

前記ソフトウェアのライセンス発行要求に応じて、暗号化された状態で提供される前記ソフトウェアを復号するためのソフトウェア復号キーを前記着脱キー固有暗号キーで暗号化して、暗号化された前記ソフトウェア復号キーを含むライセンス情報を出力する、

処理を実行させることを特徴とするライセンス発行プログラムを記録したコンピュータ読み取り可能な記録媒体。

#### 【0286】

##### 【発明の効果】

以上説明したように本発明の第1、第2の態様では、ソフトウェア復号キーを装置識別情報で暗号化しているため、その装置識別情報が固定的に記録された処理装置でのみ暗号化されたソフトウェアを復号することが可能となる。その結果、他の装置にソフトウェアを読み込ませても、その装置でそのソフトウェアを実行することができず、ソフトウェアの不正使用が防止される。

#### 【0287】

また、本発明の第3、第4の態様では、正しいハードウェアキーが装着された処理装置に限りライセンス情報を復号し、暗号化された状態のソフトウェアを復号することができる。しかも、装置識別情報がハードウェアキーに格納されていることにより、装置識別情報が合致する処理装置でのみソフトウェアを復号できる。

##### 【図面の簡単な説明】

##### 【図1】

第1の実施の形態に適用される発明の概念図である

##### 【図2】

第1の実施の形態のシステム構成例を示す図である。

**【図 3】**

本発明の実施の形態に用いるソフトウェア提供サーバのハードウェア構成例を示す図である。

**【図 4】**

第 1 の実施の形態に係るソフトウェアライセンス管理システムの機能ブロック図である。

**【図 5】**

第 1 の実施の形態におけるソフトウェア暗号化処理を示すシーケンス図である。

**【図 6】**

第 1 の実施の形態におけるソフトウェア提供処理を示すシーケンス図である。

**【図 7】**

第 2 の実施の形態に適用される発明の概念図である。

**【図 8】**

第 2 の実施の形態に係るライセンス管理システムの概念図である。

**【図 9】**

第 2 の実施の形態におけるライセンス管理機構の概念図である。

**【図 10】**

処理装置のハードウェア構成例を示す図である。

**【図 11】**

プロセッサカートリッジのハードウェア構成例を示す図である。

**【図 12】**

各サーバコンピュータの処理機能を示すブロック図である。

**【図 13】**

着脱キーに格納される着脱キー情報のデータ構造例を示す図である。

**【図 14】**

着脱キー発行記録データベースのデータ構造例を示す図である。

**【図 15】**

アプリケーション登録記録データベースのデータ構造例を示す図である。

**【図 16】**

アプリケーション実行ライセンスのデータ構造例を示す図である。

**【図 17】**

ライセンス情報データベースのデータ構造例を示す図である。

**【図 18】**

ライセンス発行記録データベースのデータ構造例を示す図である。

**【図 19】**

ハードウェアキー生成処理の概念図である。

**【図 20】**

着脱キー情報発行部の処理手順を示すフローチャートである。

**【図 21】**

アプリケーション処理の概念図である。

**【図 22】**

アプリケーション暗号／復号キー発行部の処理手順を示すフローチャートである。

**【図 23】**

アプリケーションの暗号化前後の状態を示す図である。

**【図 24】**

アプリケーション暗号化処理手順を示すフローチャートである。

**【図 25】**

ライセンス提供処理の概念図である。

**【図 26】**

ライセンス発行部の処理手順を示すフローチャートである。

**【図 27】**

ライセンス発行費用請求処理の手順を示すフローチャートである。

**【図 28】**

処理装置に構築される処理機能を示すブロック図である。

**【図 29】**

取得済みライセンス情報のデータ構造例を示す図である。

**【図 3 0】**

アプリケーション稼働情報のデータ構造例を示す図である。

**【図 3 1】**

アプリケーション起動処理の手順を示すフローチャートである。

**【図 3 2】**

アプリケーションプログラム復号処理の手順を示すフローチャートである。

**【図 3 3】**

アプリケーション終了時の処理手順を示すフローチャートである。

**【図 3 4】**

アプリケーション実行継続監視処理の手順を示すフローチャートである。

**【図 3 5】**

ライセンス管理マネージャの処理手順を示す第 1 のフローチャートである。

**【図 3 6】**

ライセンス管理マネージャの処理手順を示す第 2 のフローチャートである。

**【図 3 7】**

ライセンス管理マネージャの処理手順を示す第 3 のフローチャートである。

**【図 3 8】**

ライセンス管理マネージャの処理手順を示す第 4 のフローチャートである。

**【符号の説明】**

- 1 ソフトウェア暗号キー生成手段
- 2 ソフトウェアライセンスキー生成手段
- 3 ソフトウェア暗号化手段
- 4 処理装置
  - 4 a 記録媒体
  - 4 b 装置識別情報
  - 4 c ソフトウェアライセンスキー復号手段
  - 4 d ソフトウェア復号手段
- 5 a ソフトウェア暗号キー
- 5 b ソフトウェア復号キー

---

5 c ソフトウェアライセンスキー

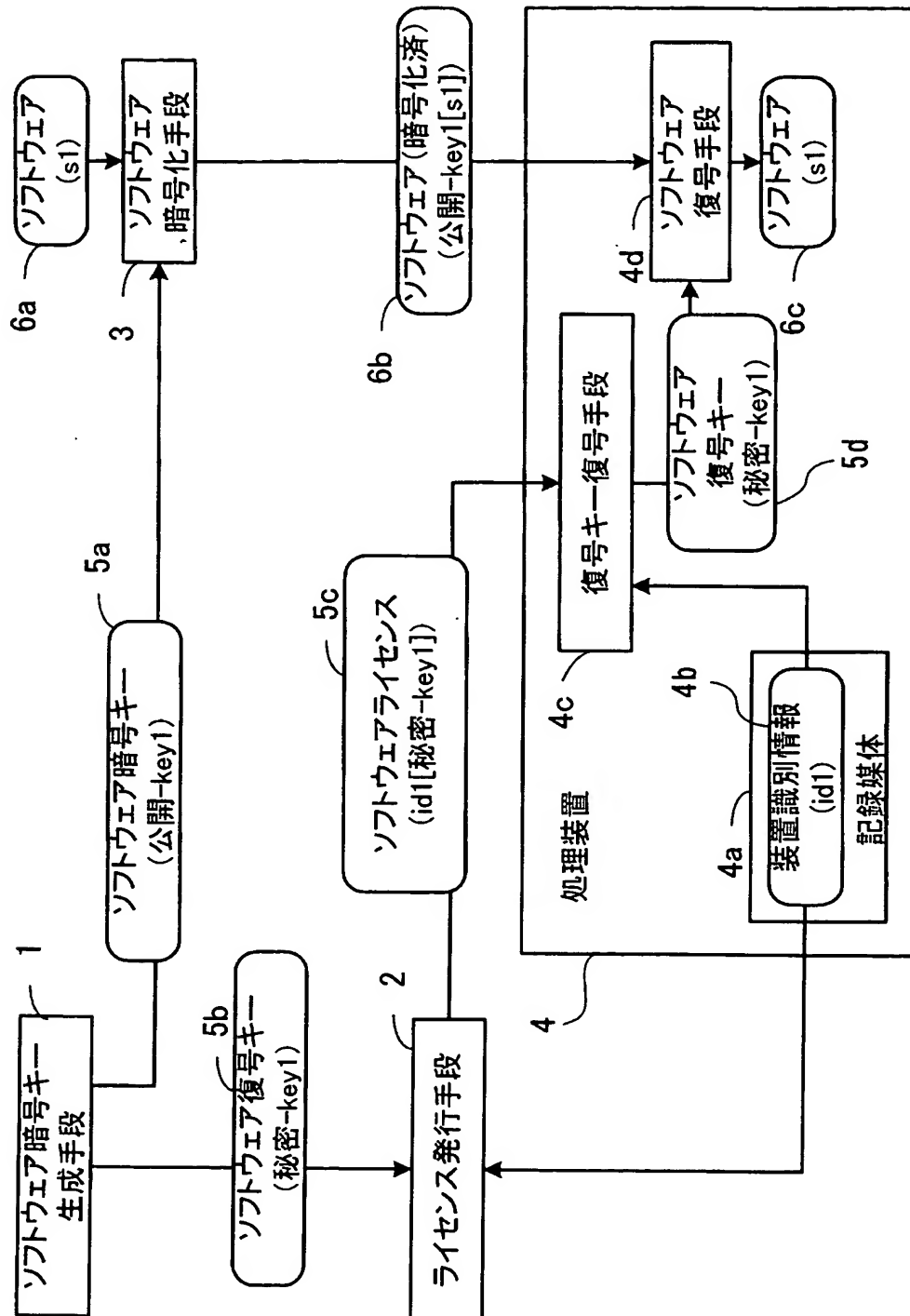
5 d ソフトウェア復号キー

6 a, 6 b, 6 c ソフトウェア

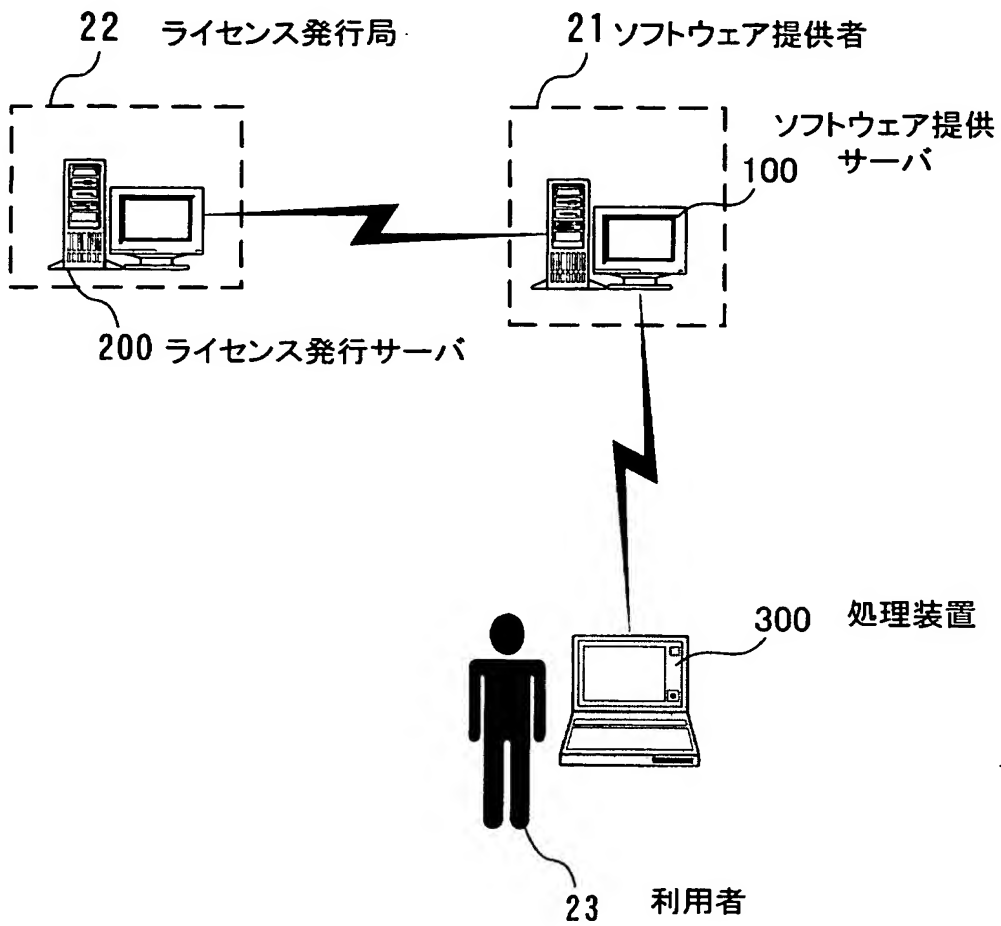
【書類名】

図面

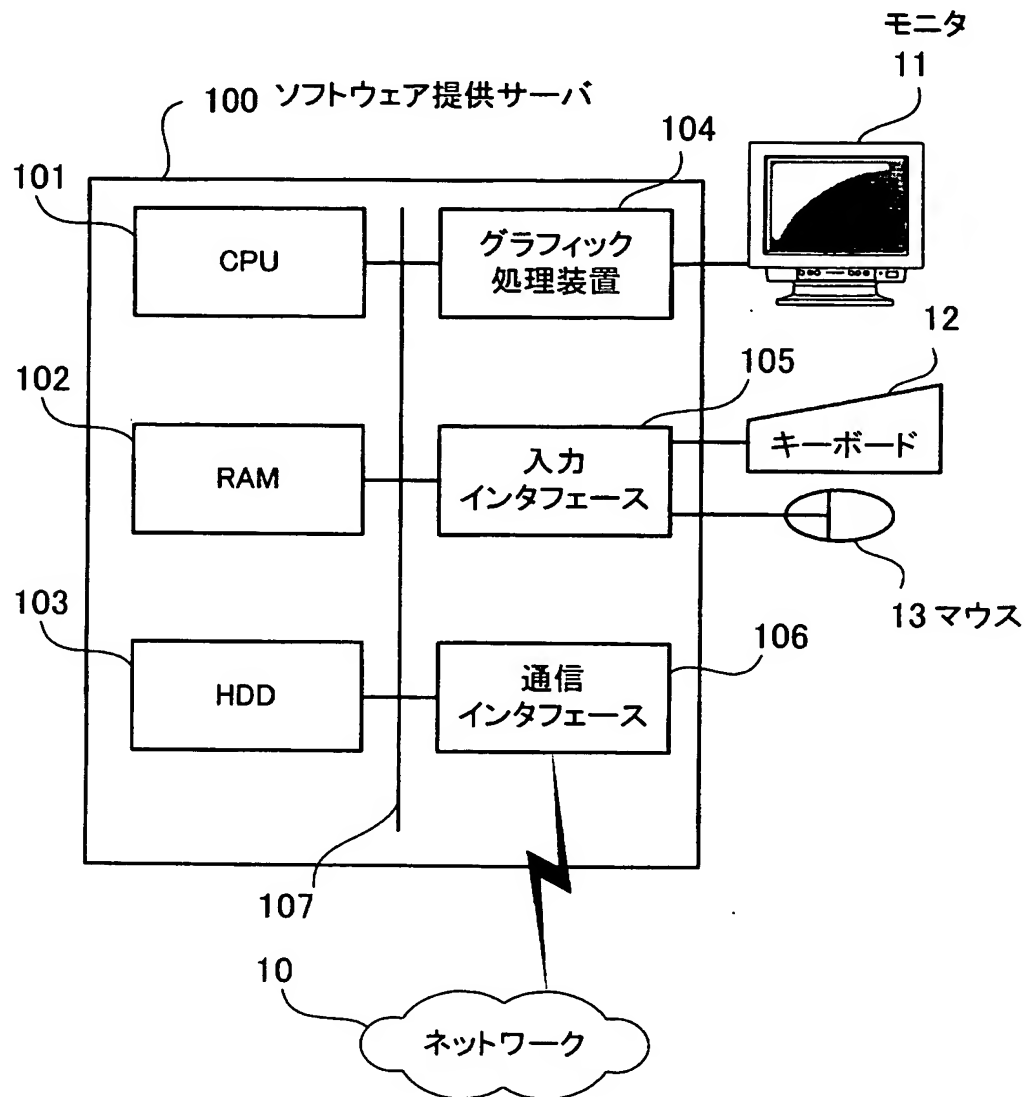
【図 1】



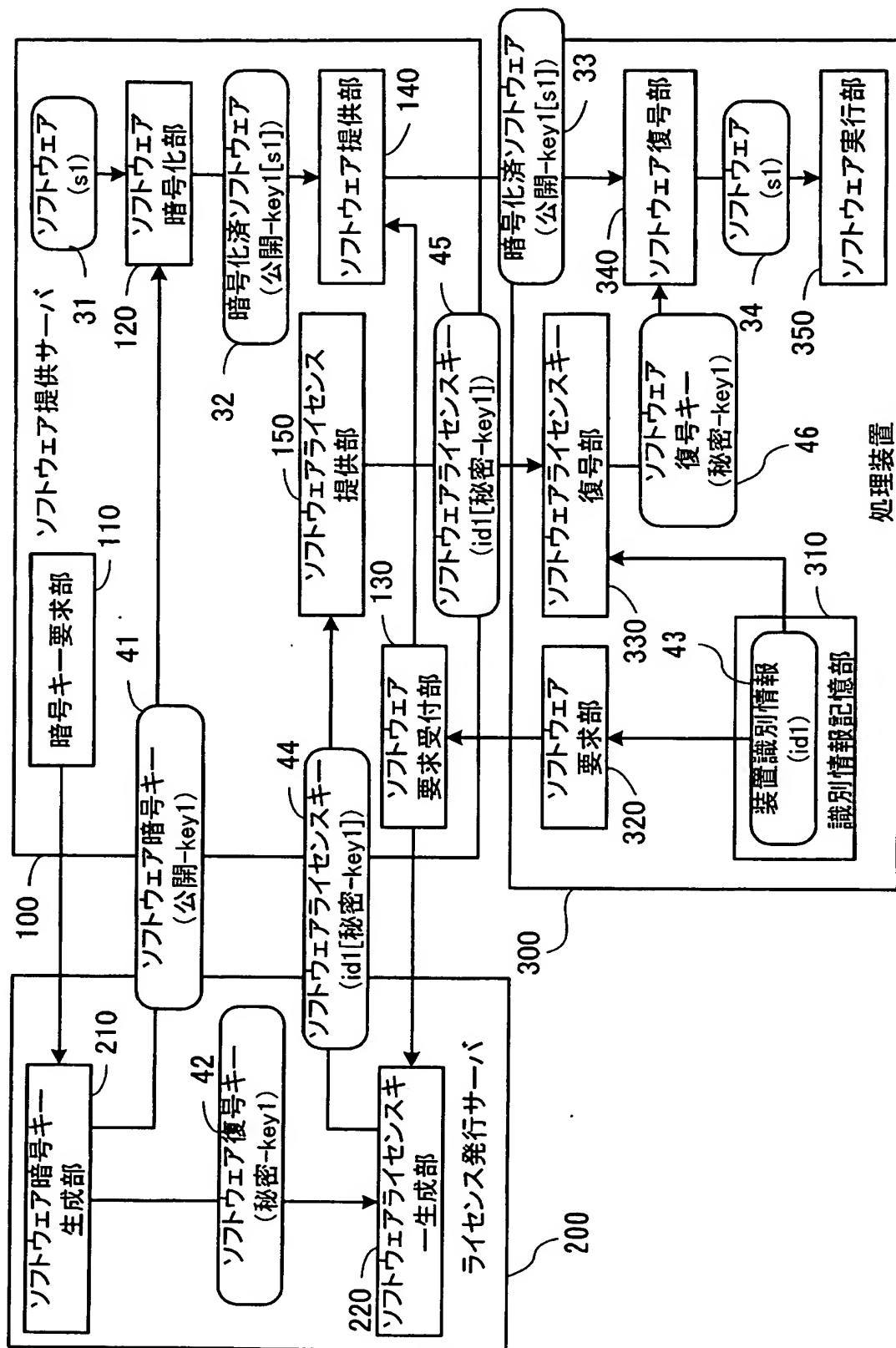
【図 2】



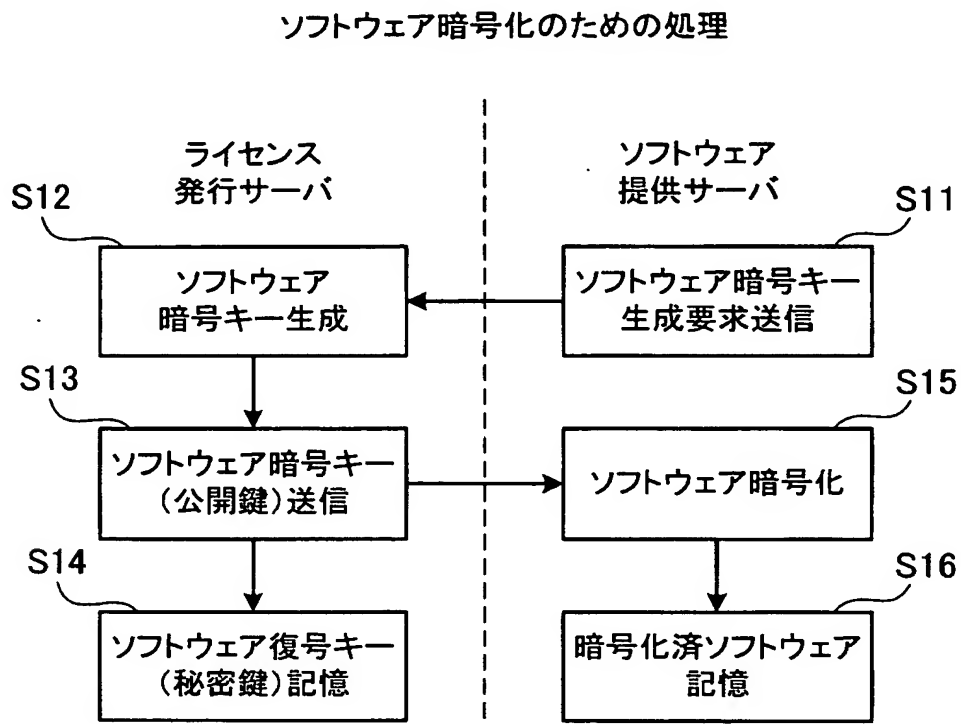
【図 3】



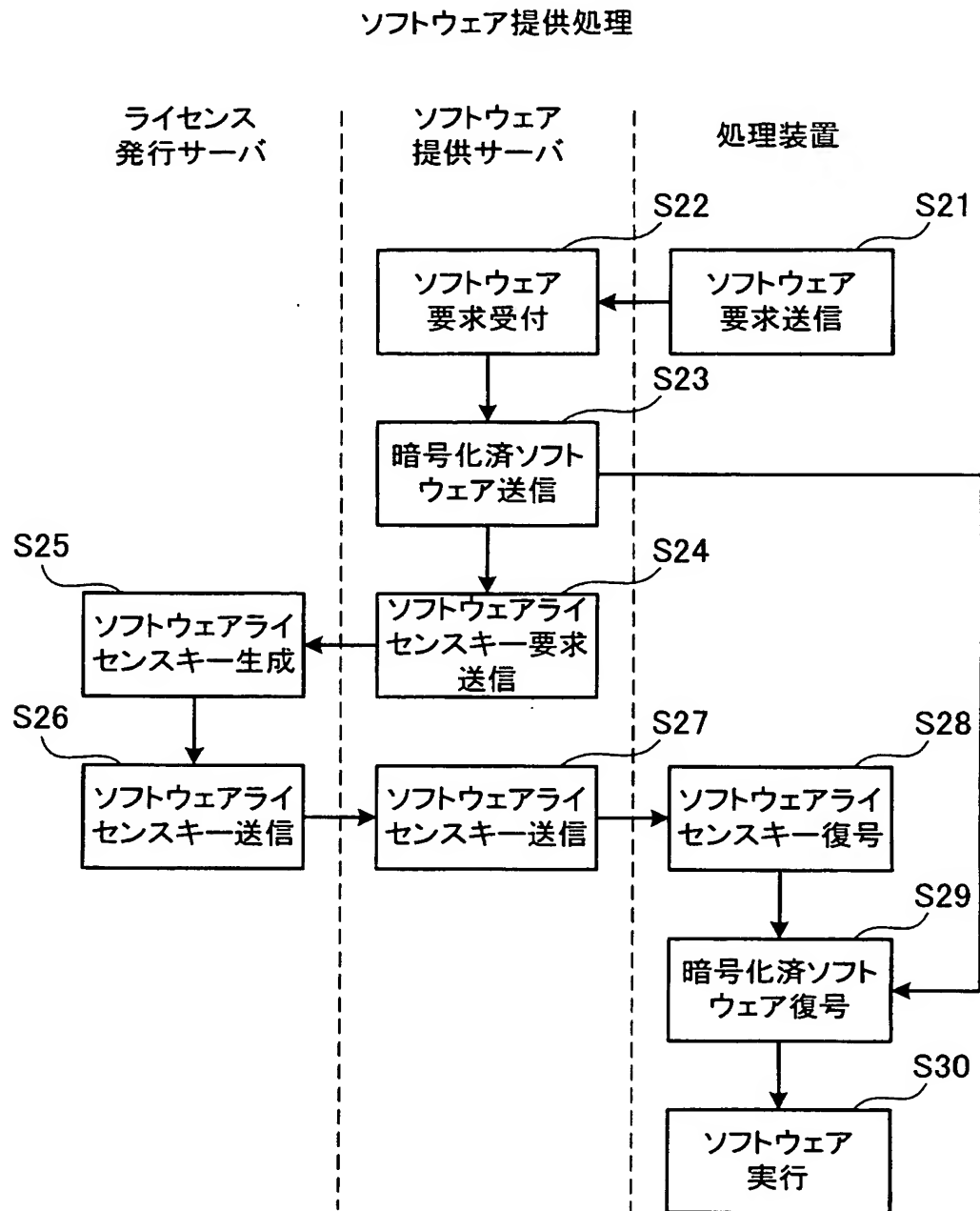
【圖 4】



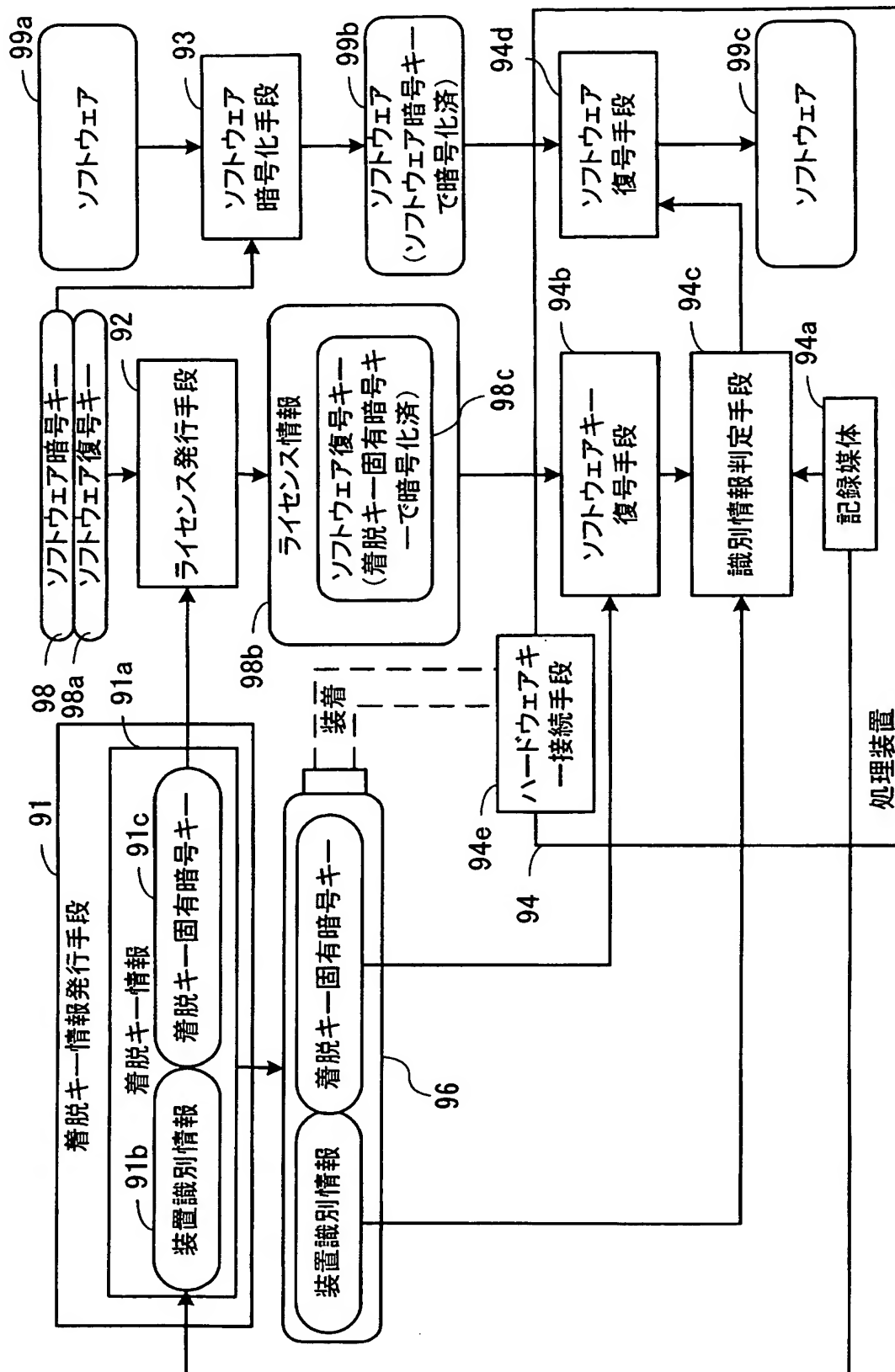
【図 5】



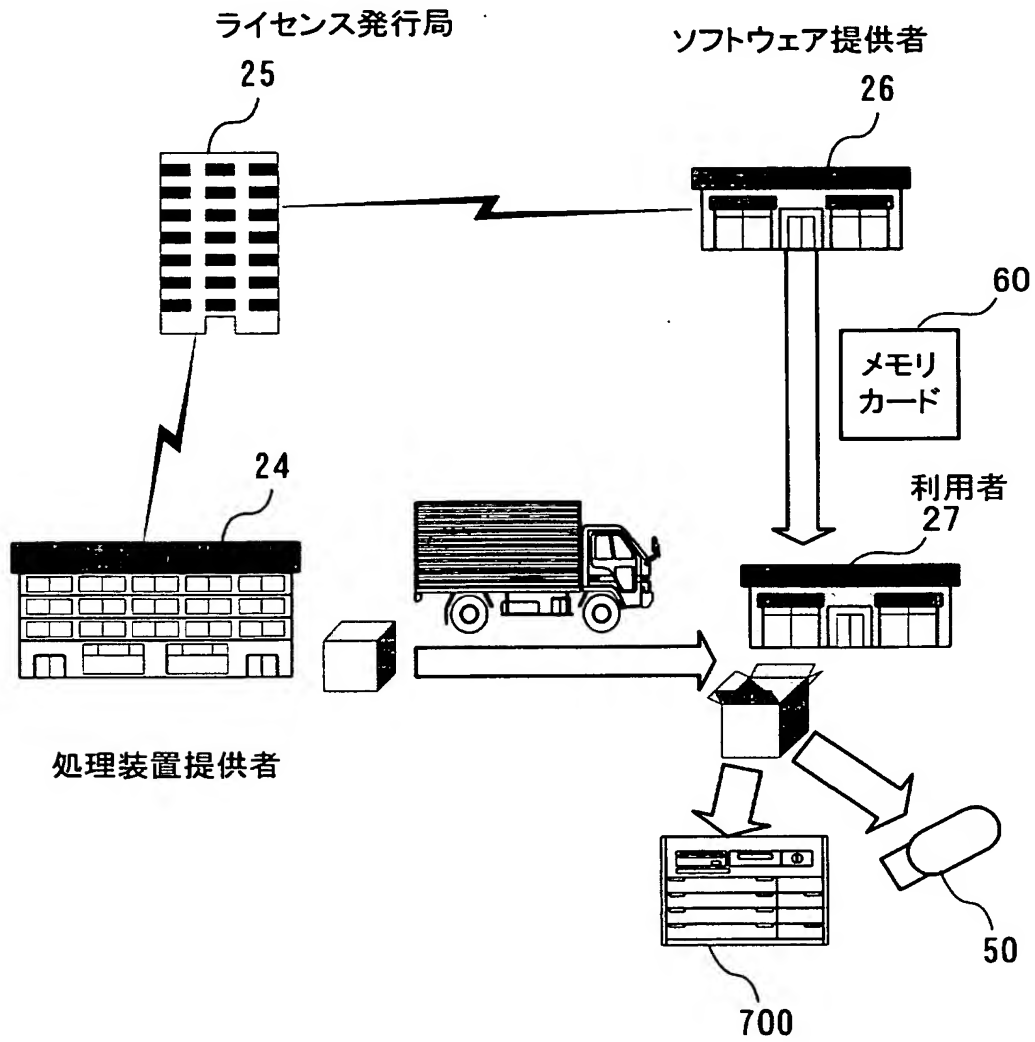
【図 6】



【图7】

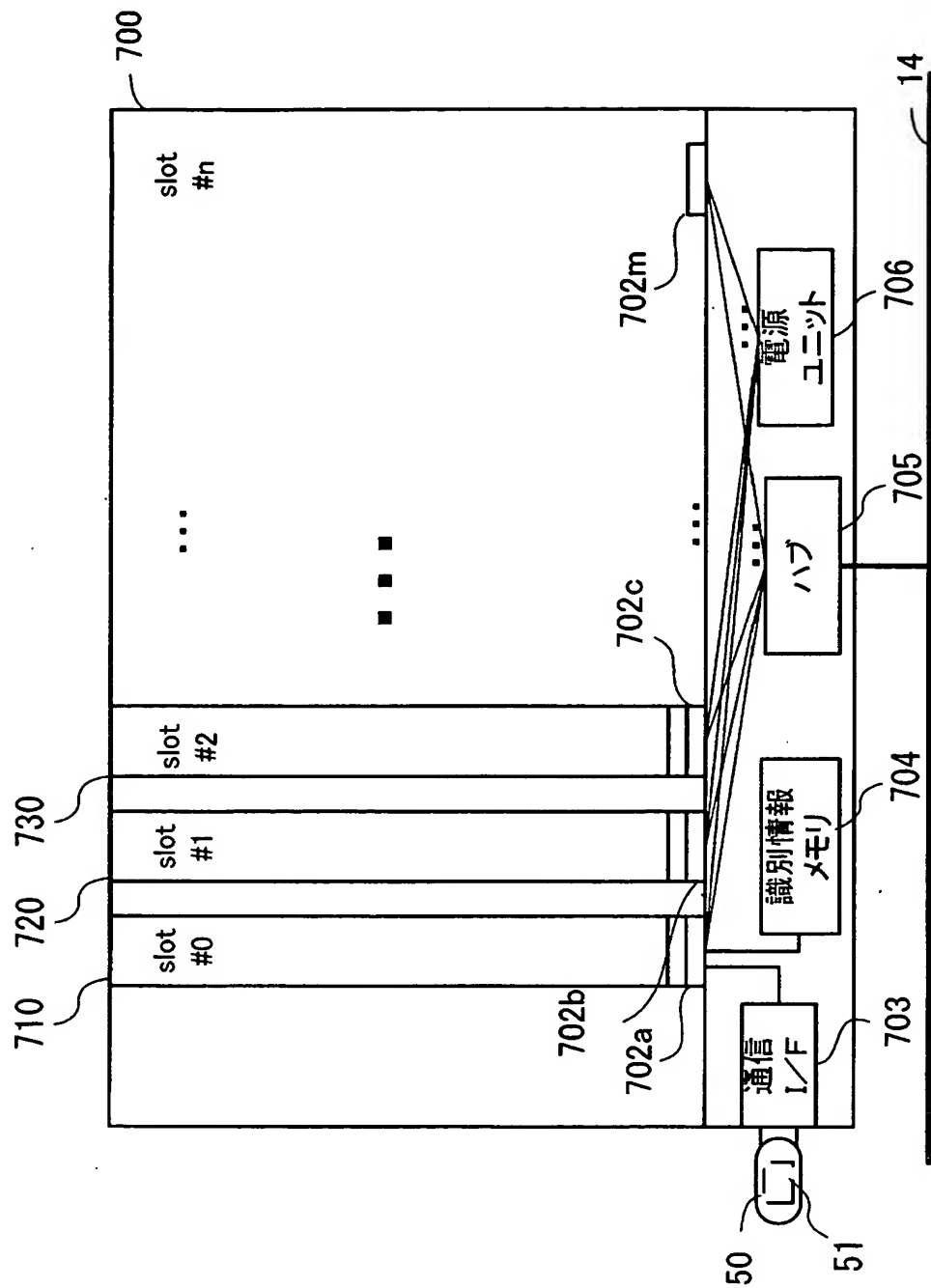


【図 8】

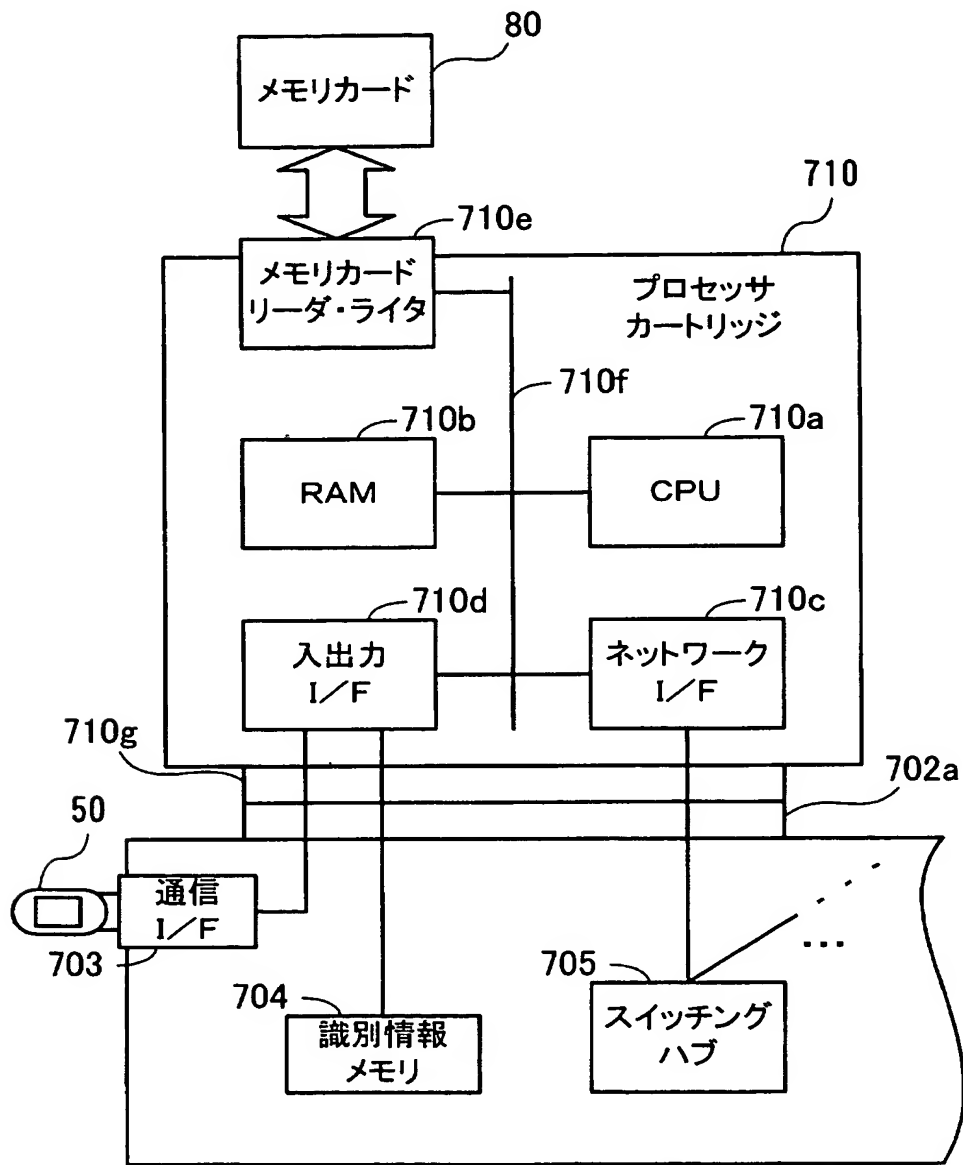




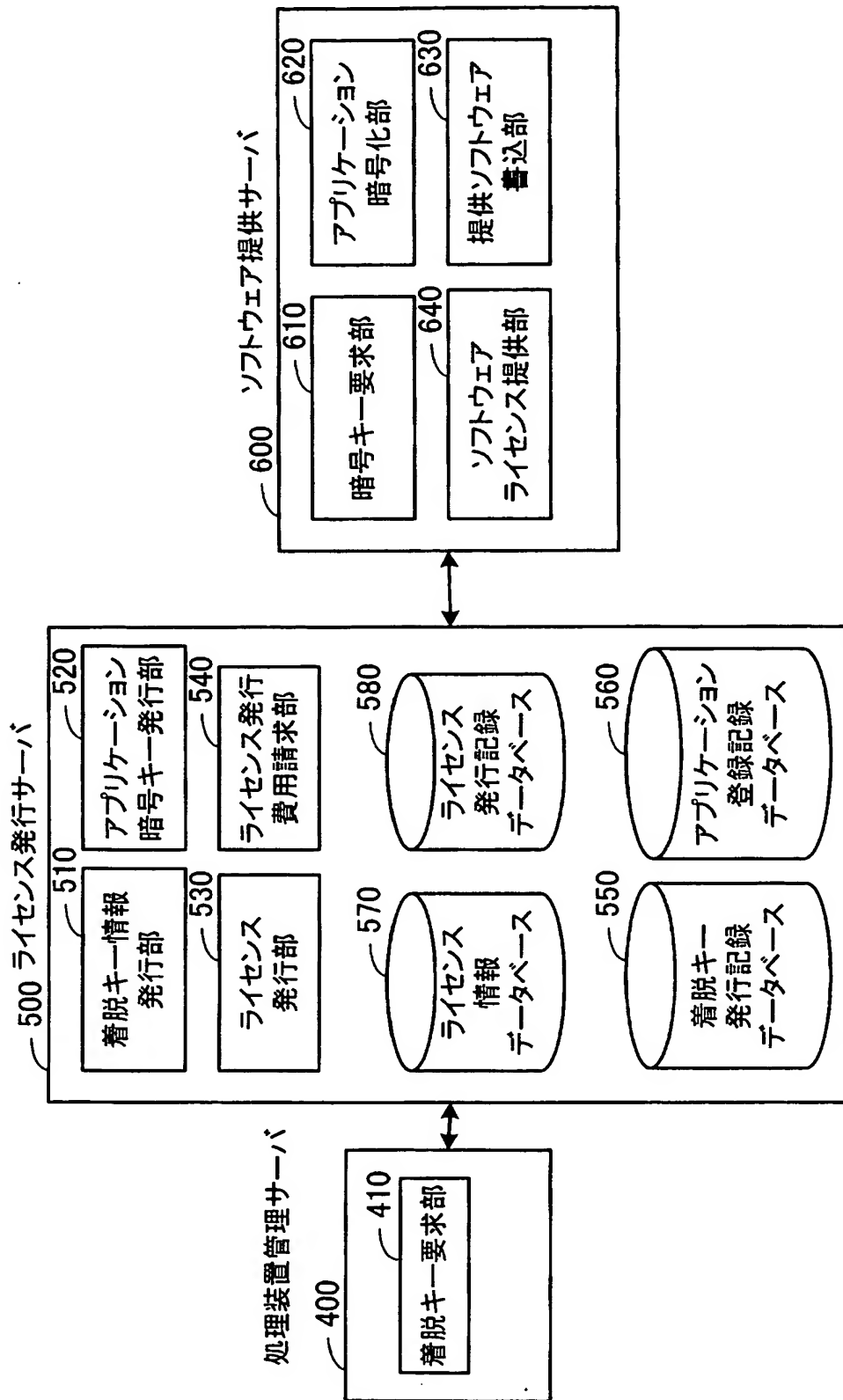
【図 10】



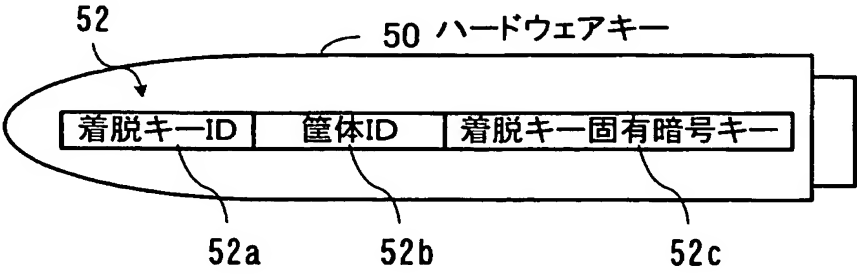
【図 11】



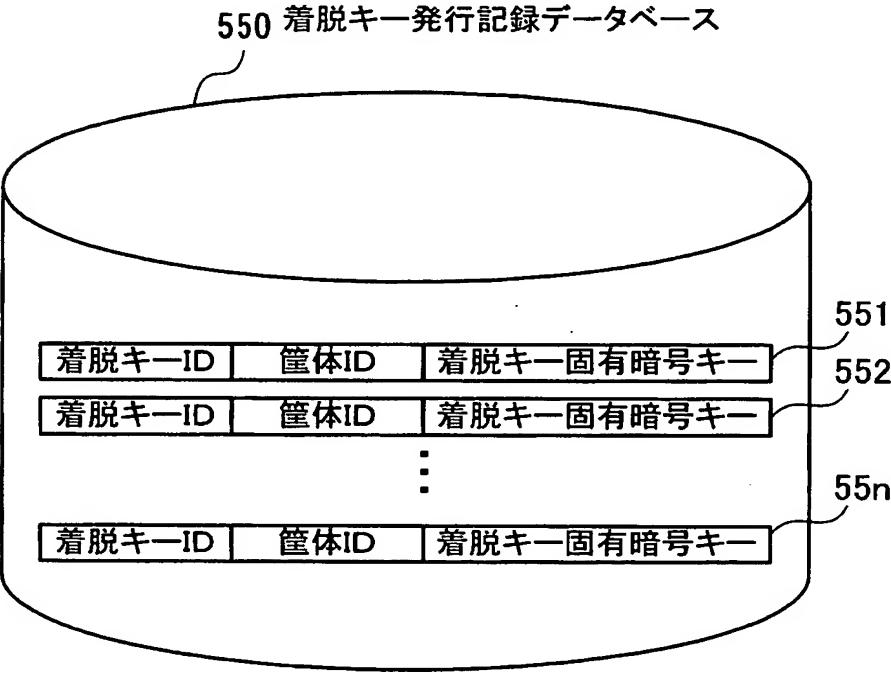
【図 12】



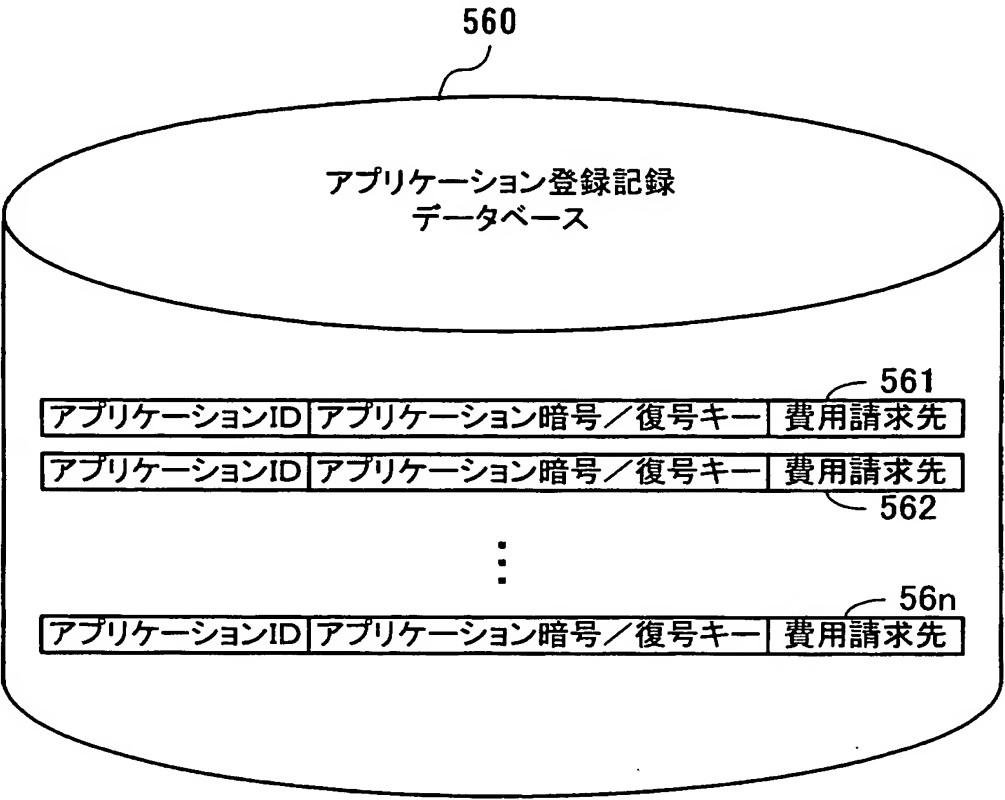
【図 1 3】



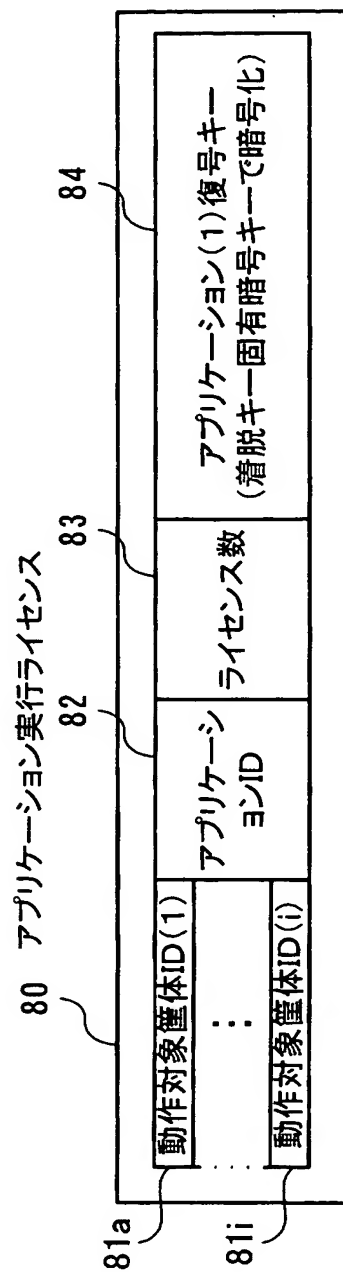
【図 1 4】



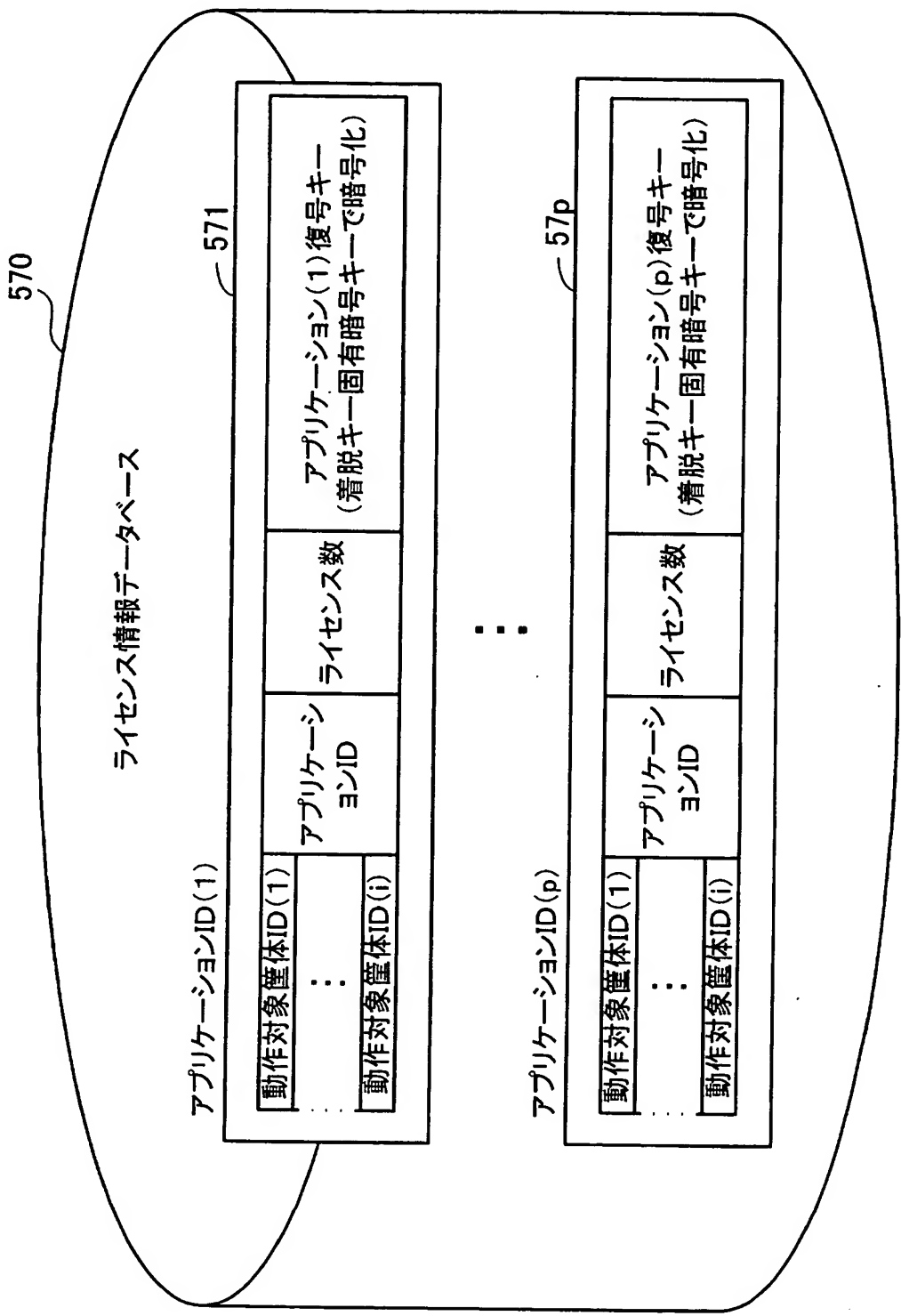
【図 15】



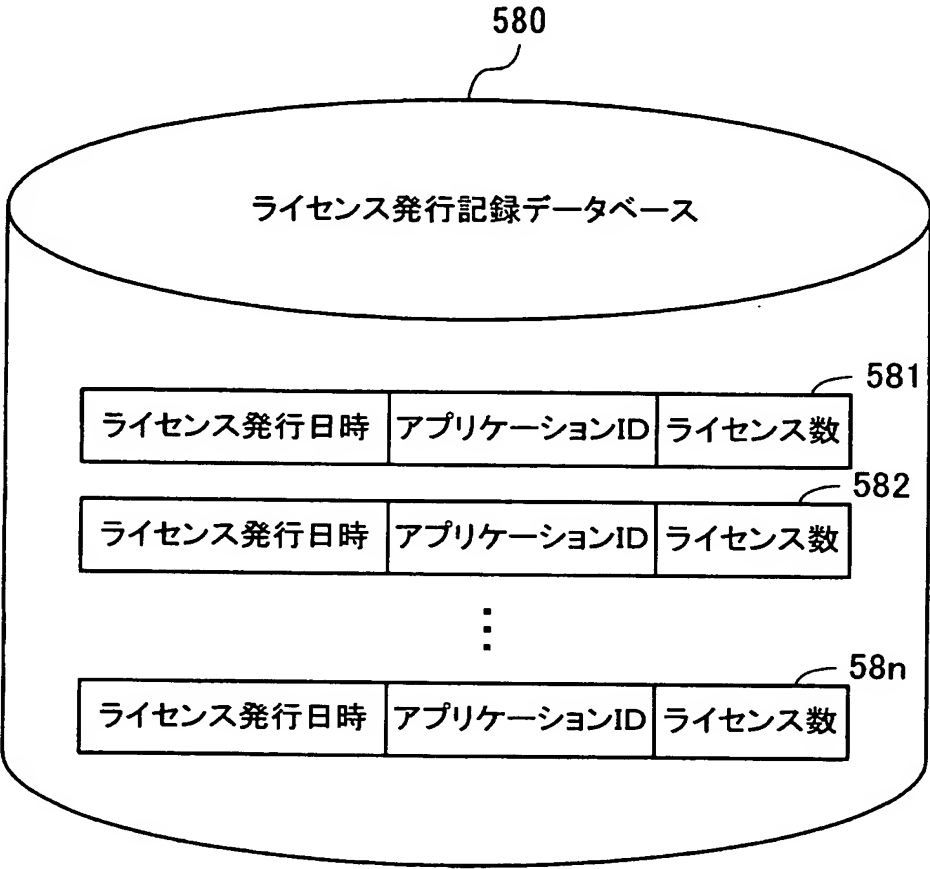
【図 16】



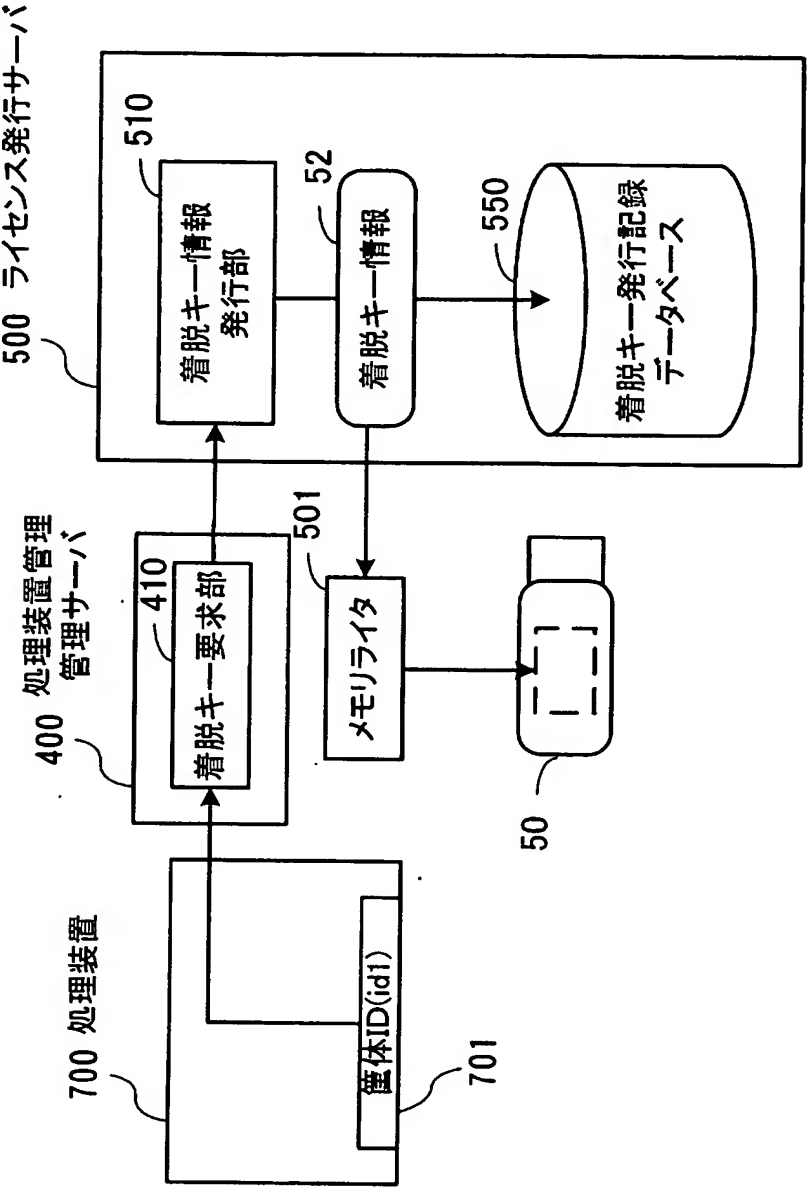
【図 17】



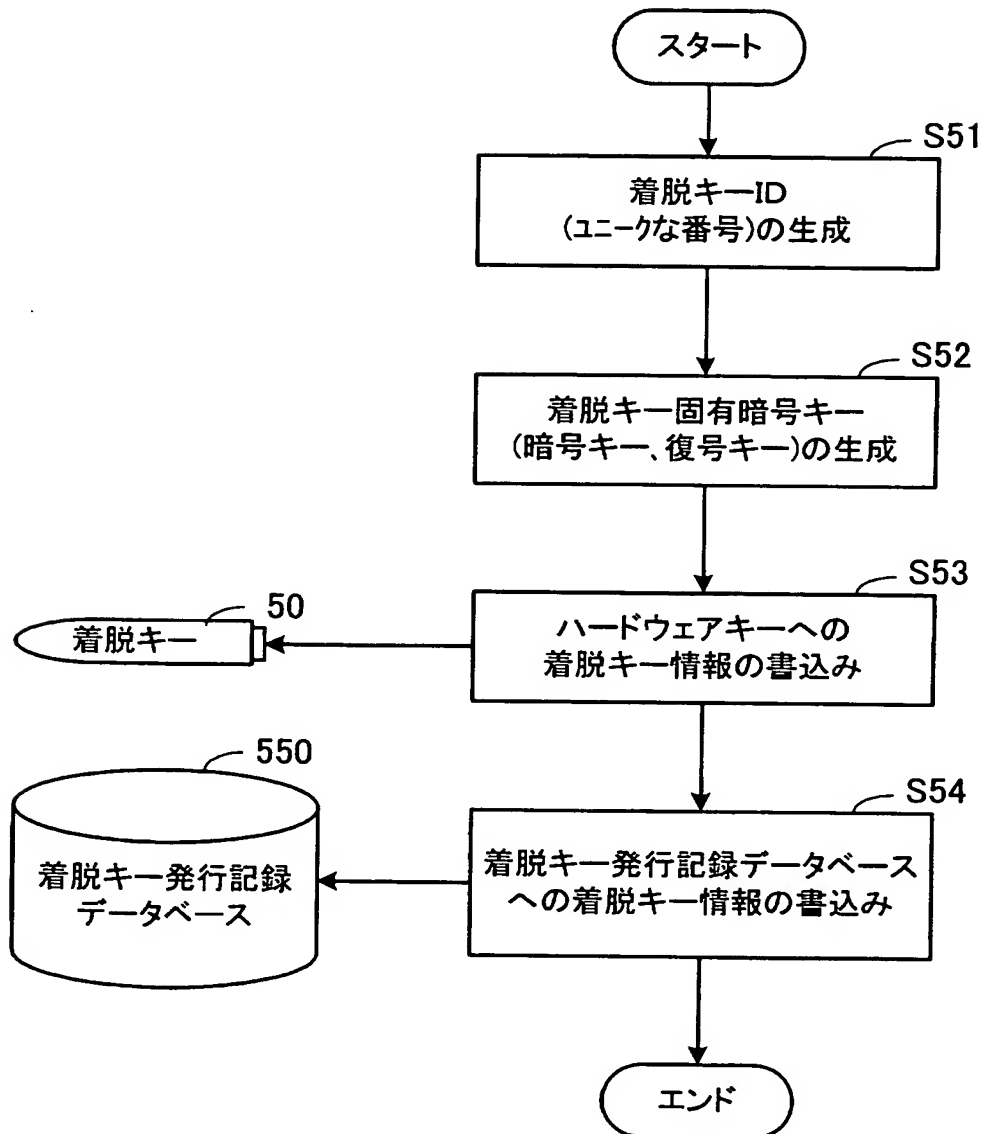
【図 18】



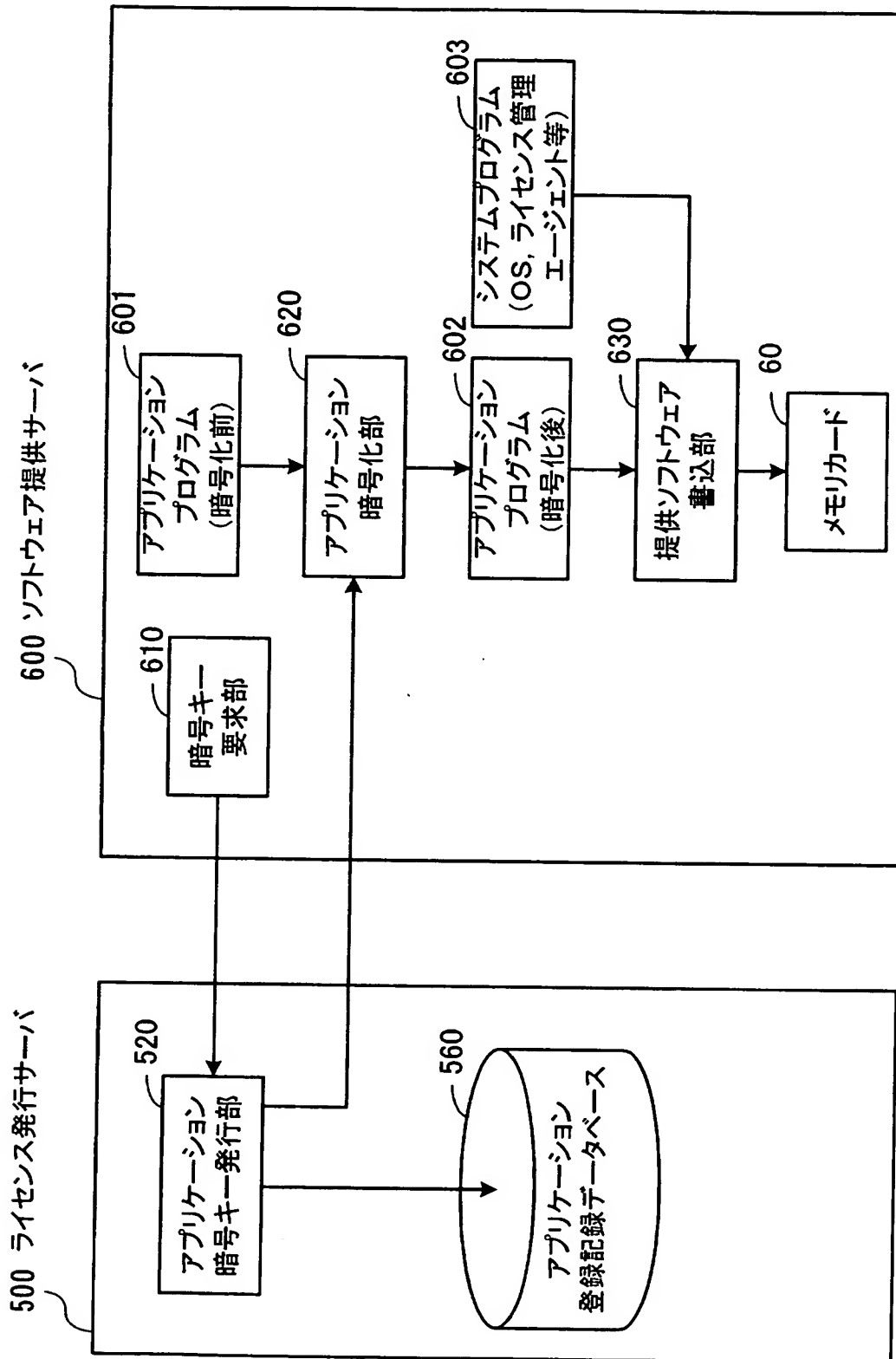
【図 19】



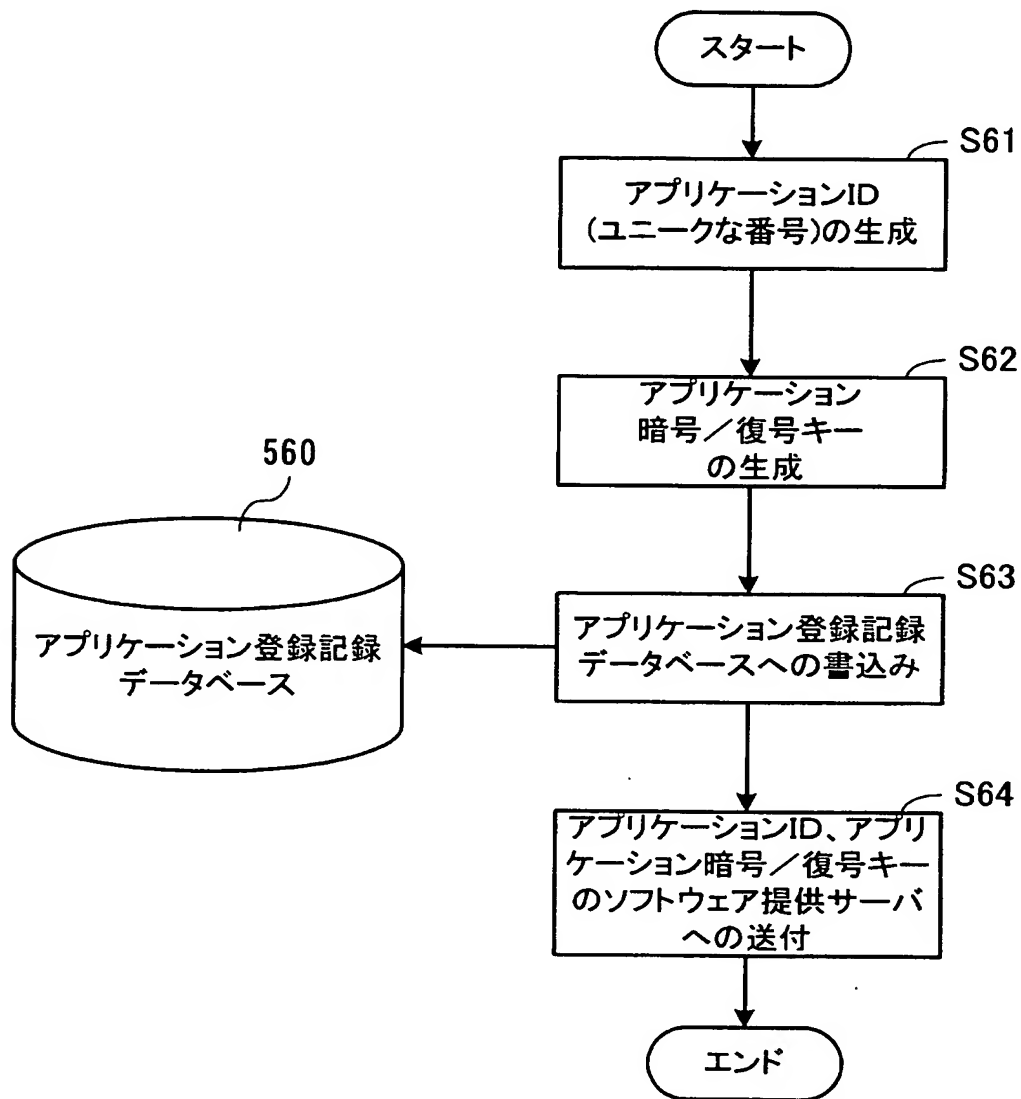
【図 20】



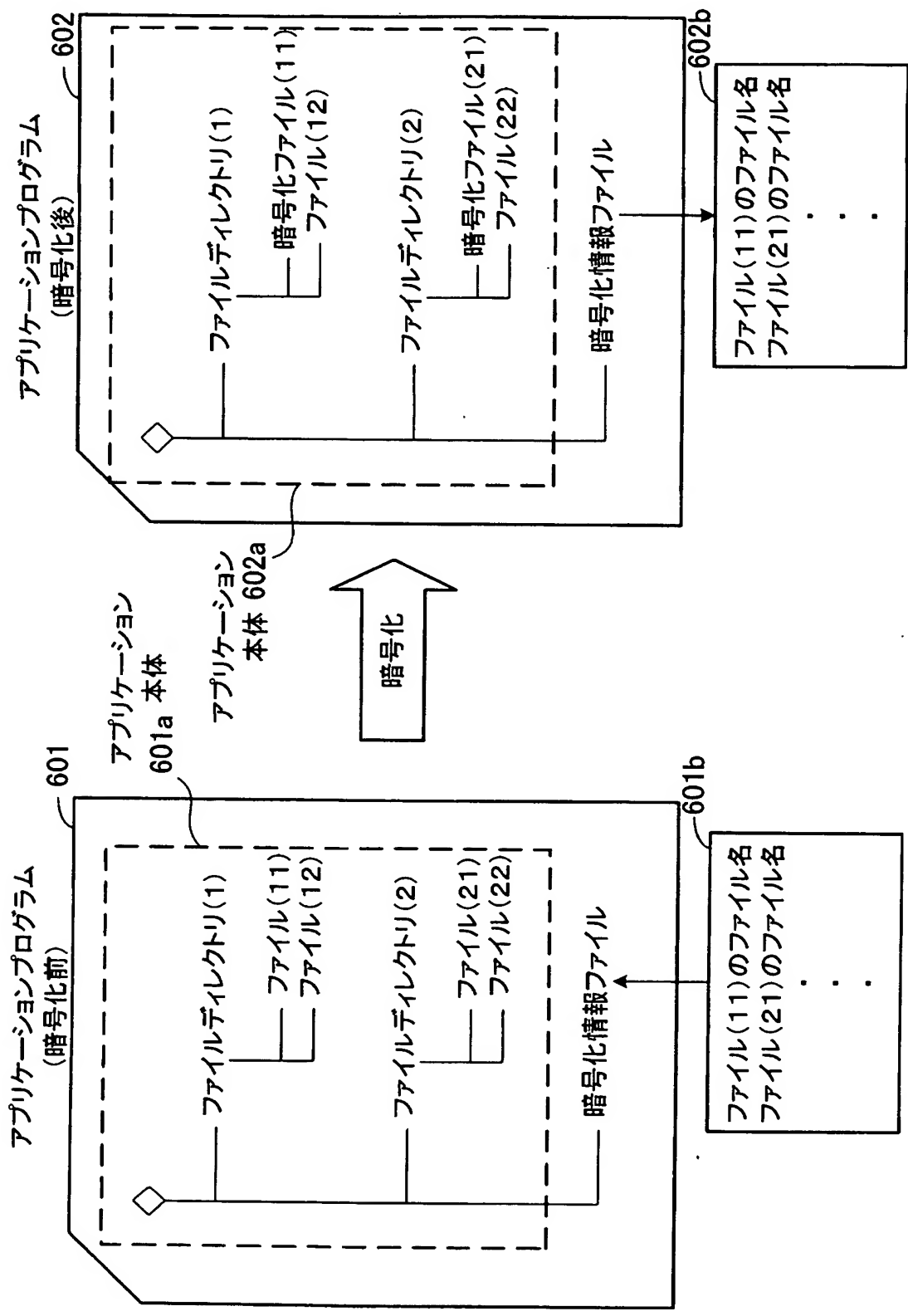
【図 21】



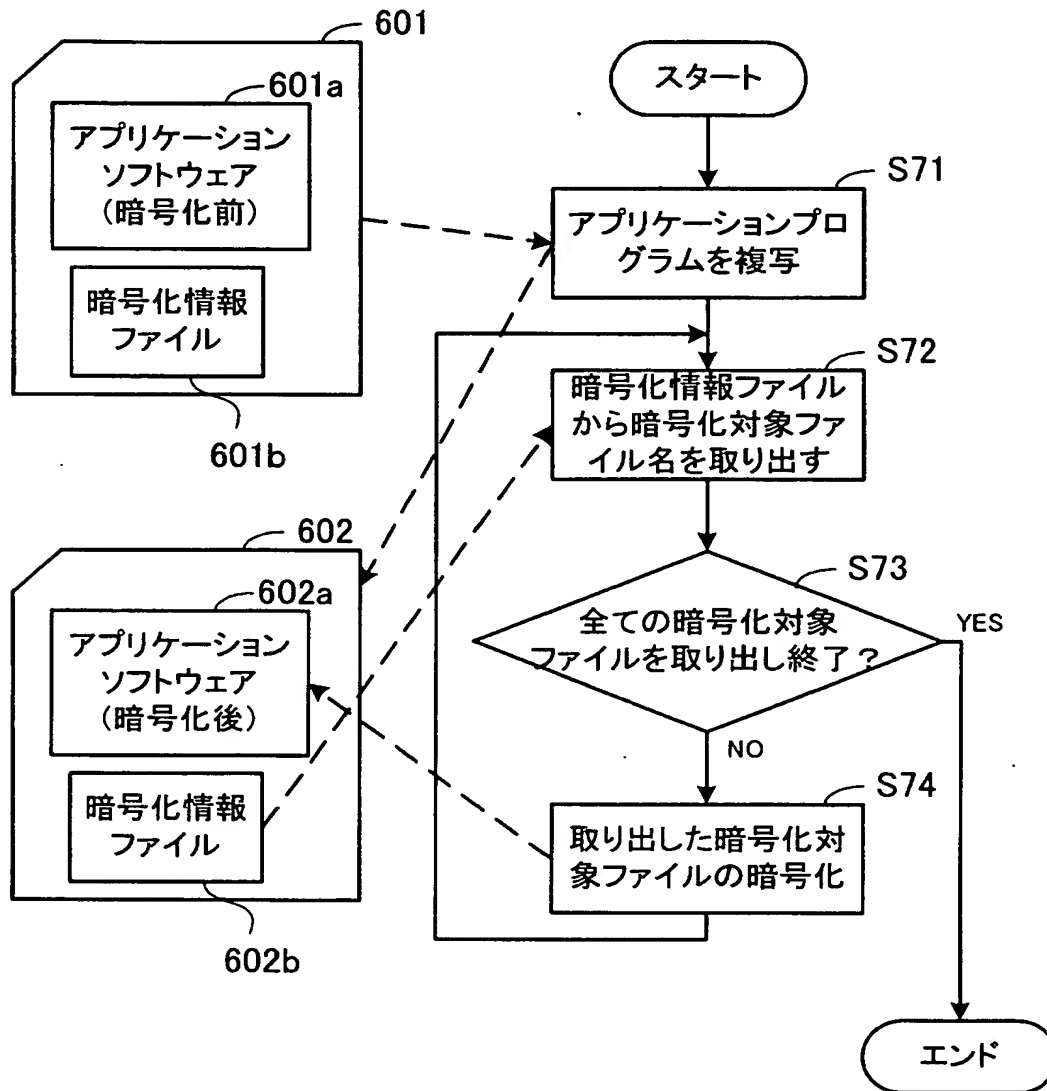
【図 22】



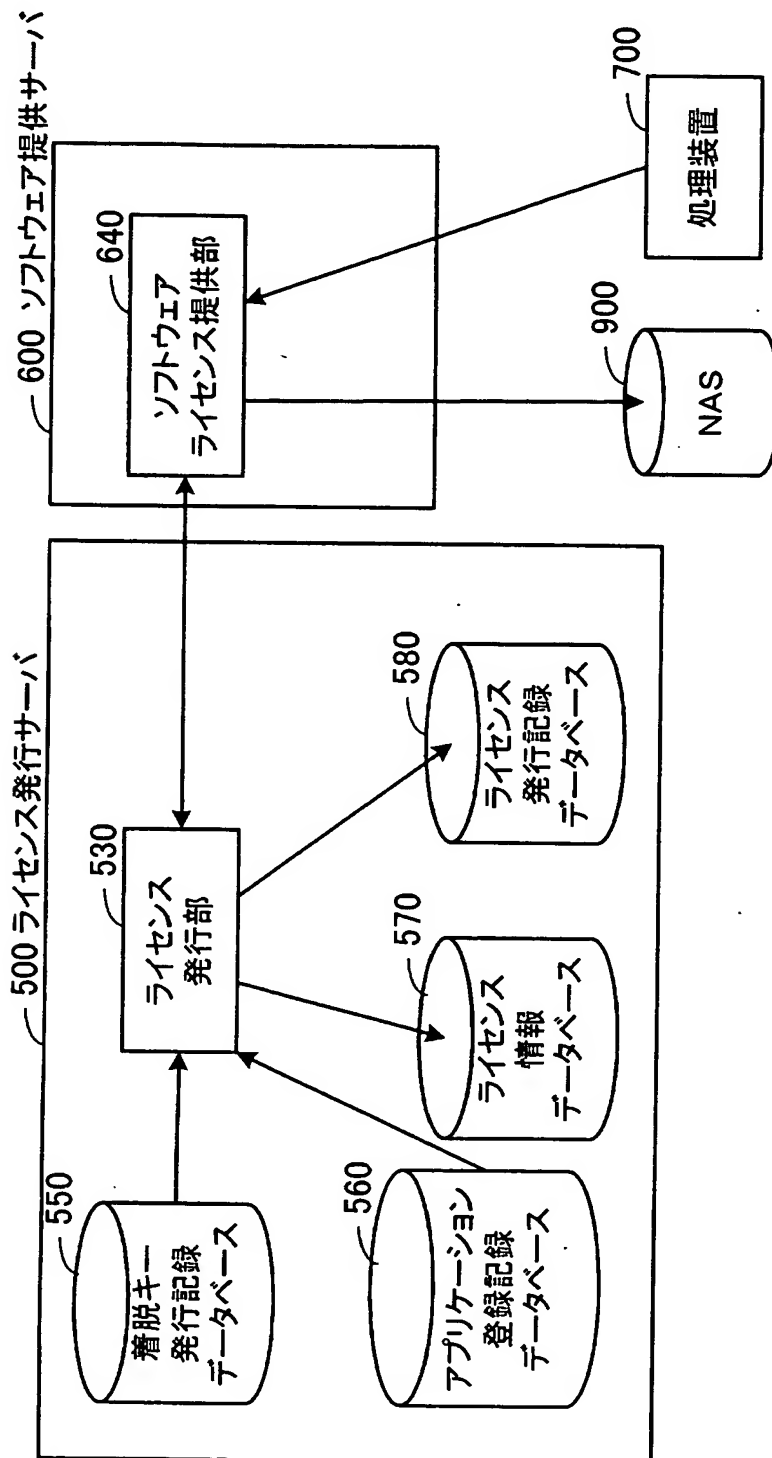
【図 23】



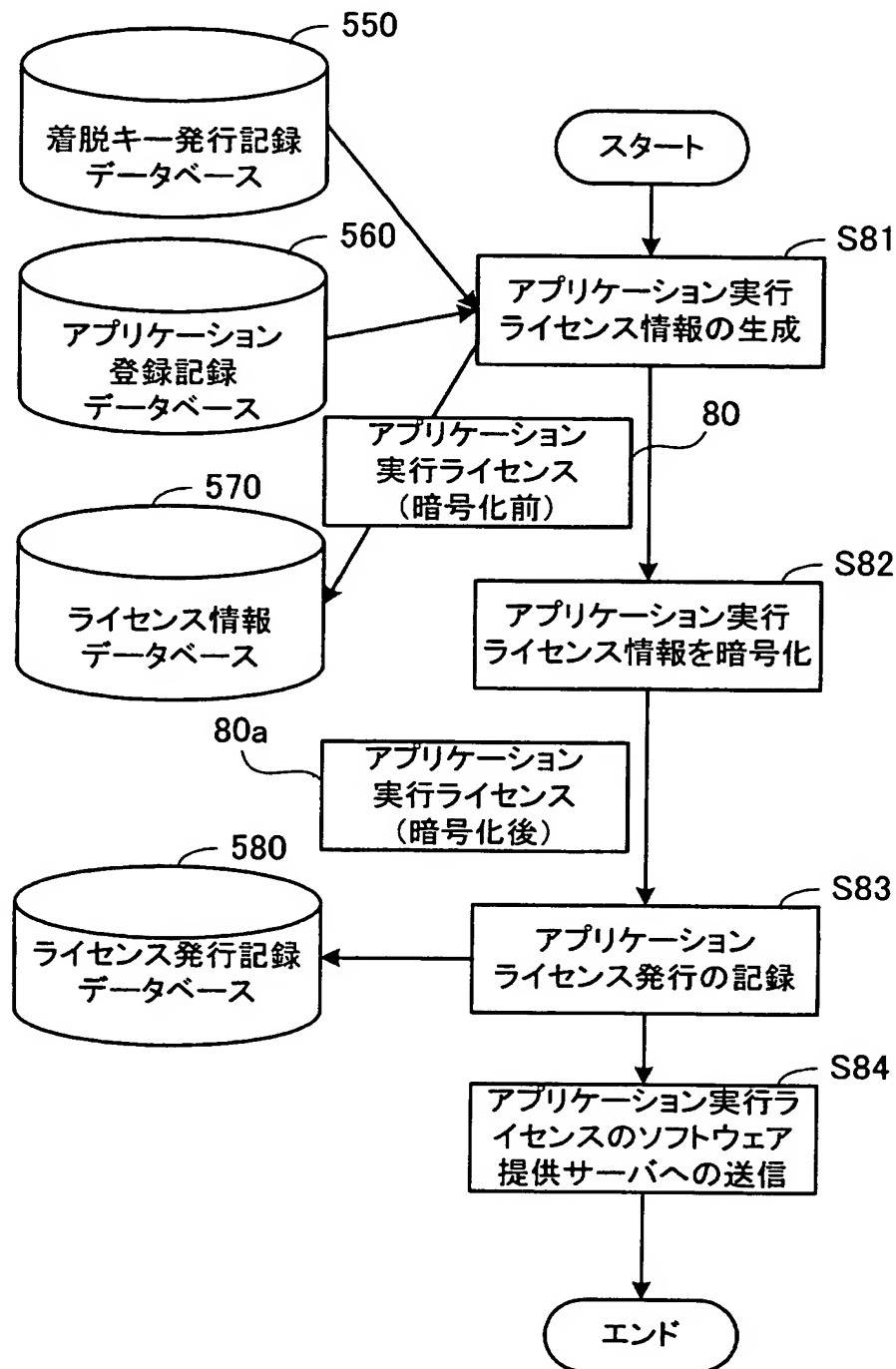
【図 24】



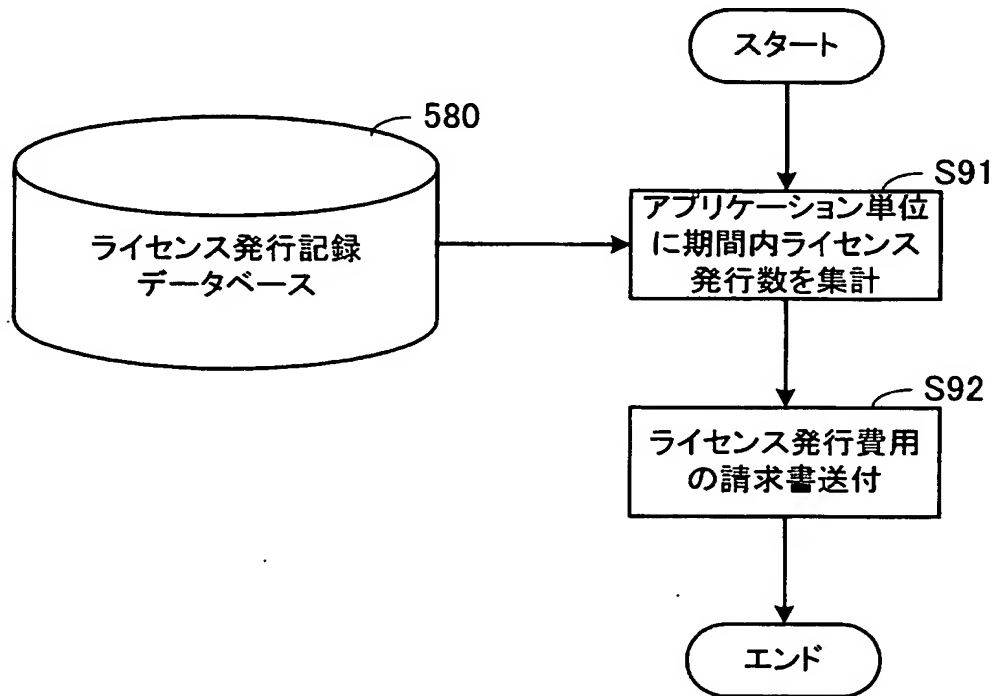
【図 25】



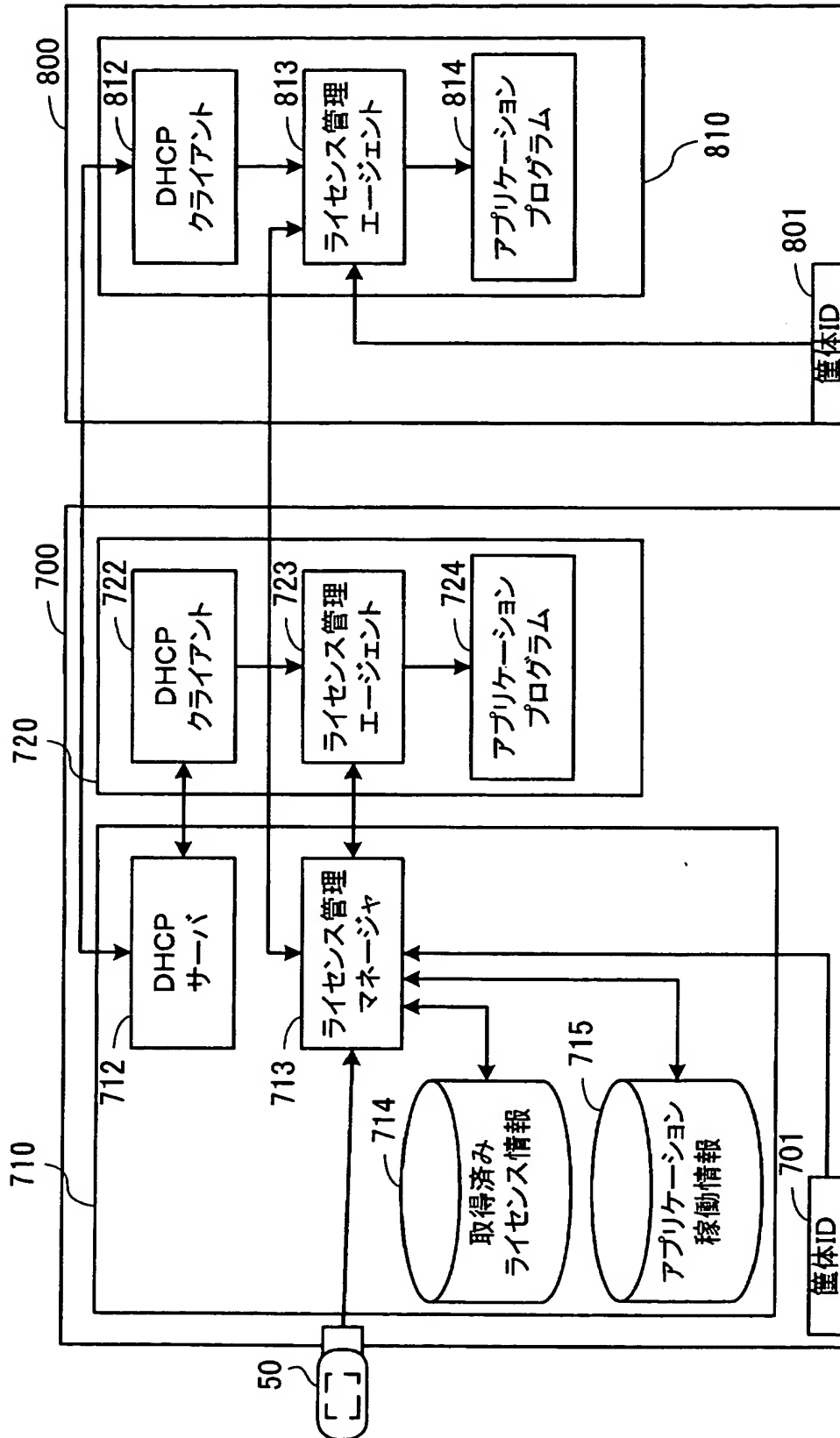
【図 26】



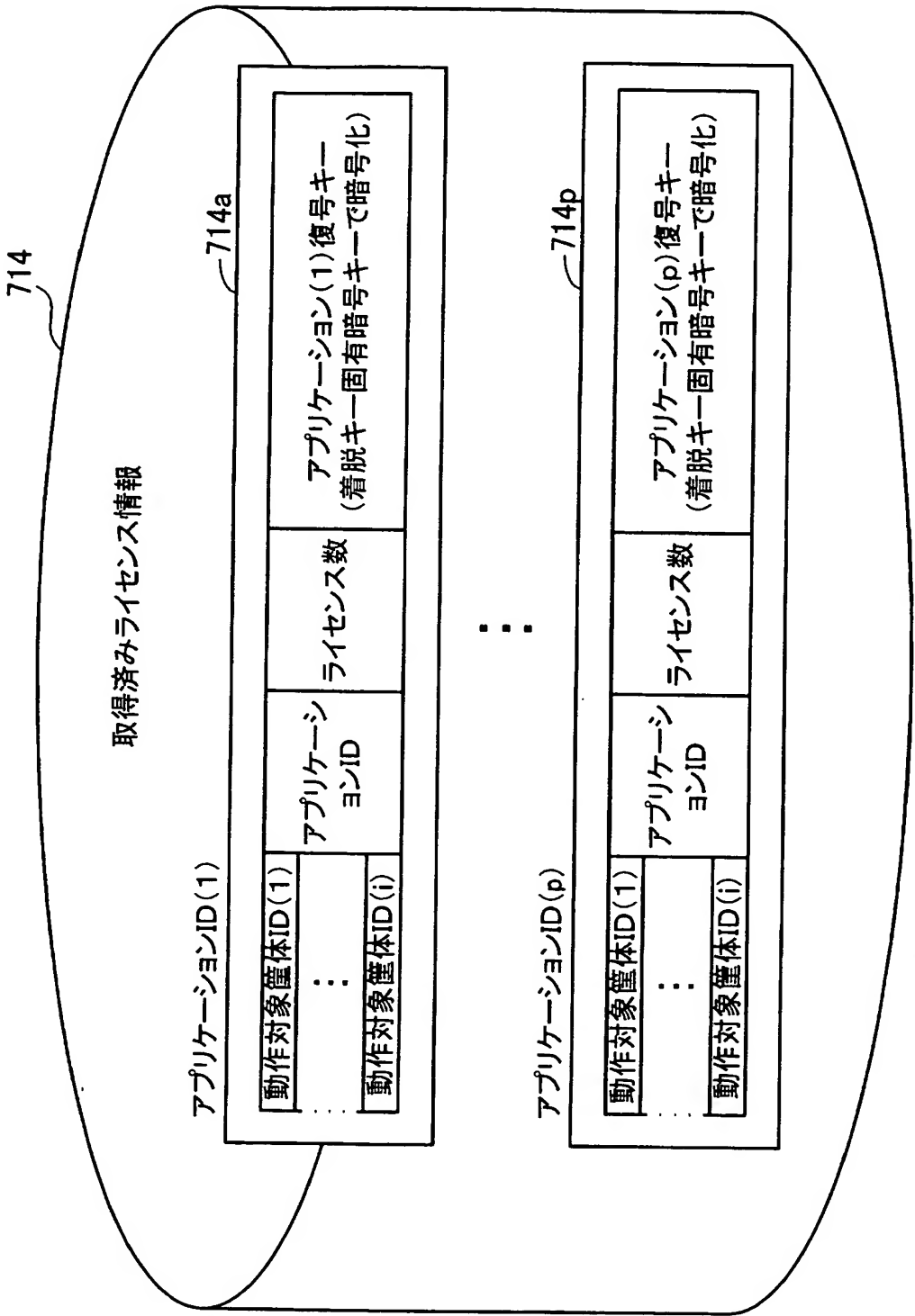
【図 27】



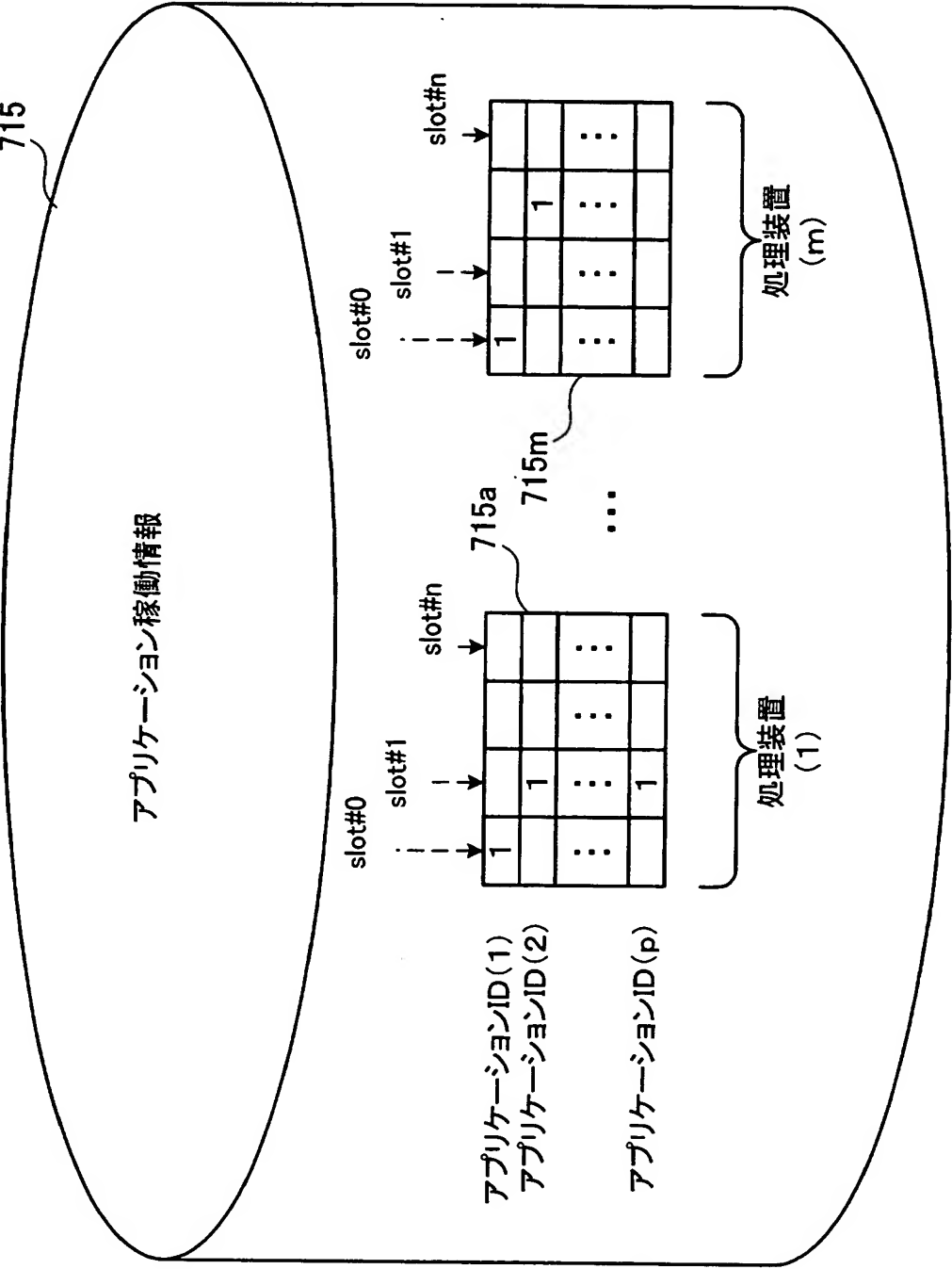
【図 28】



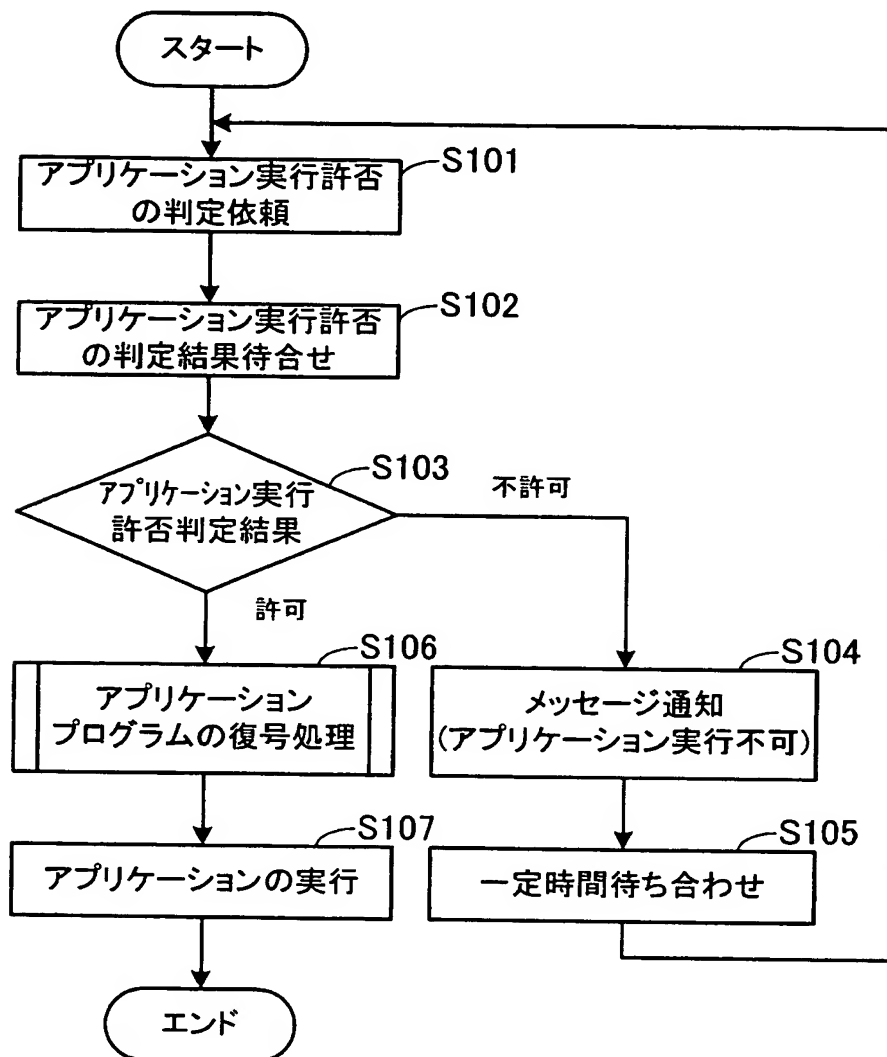
【図 29】



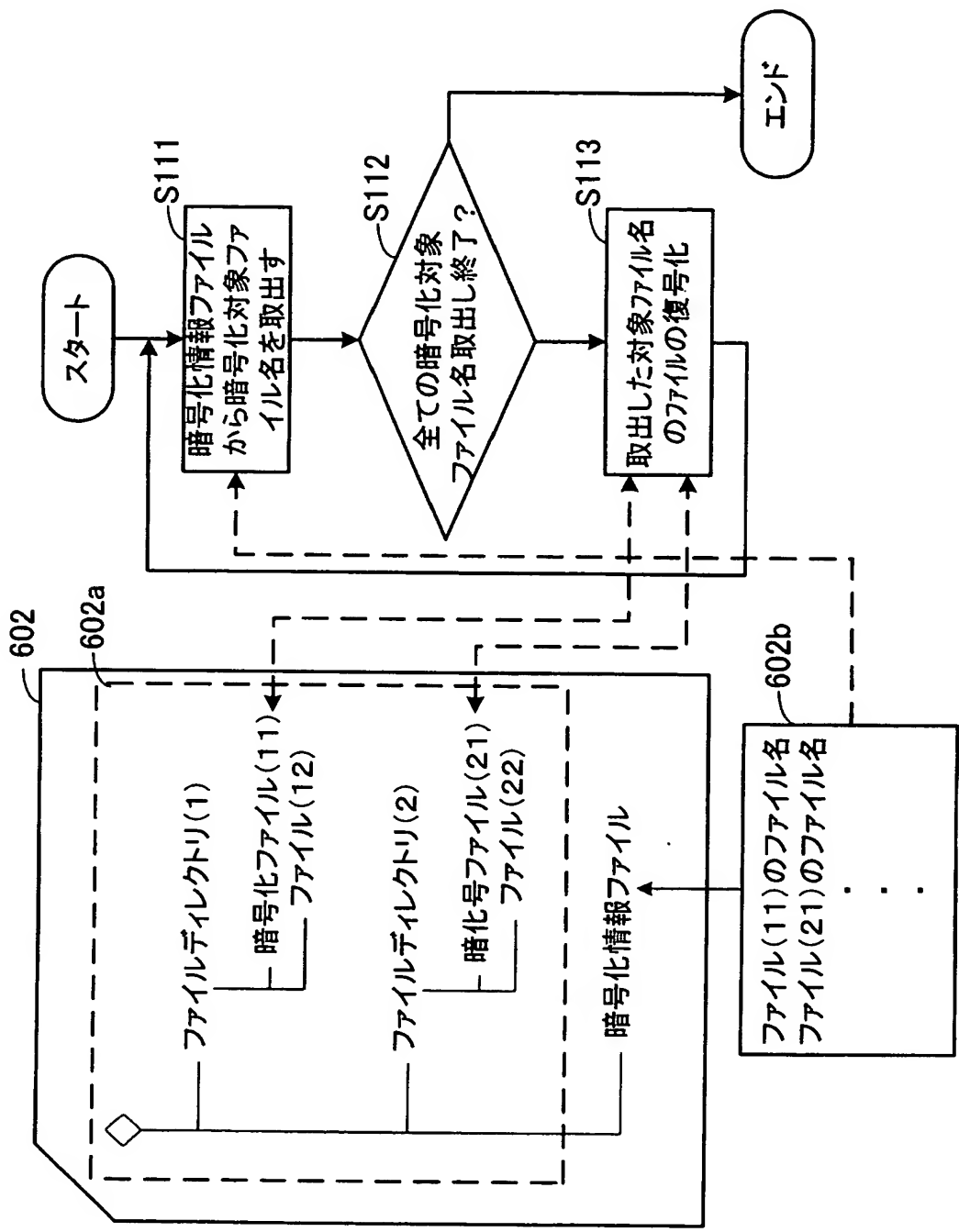
【図 30】



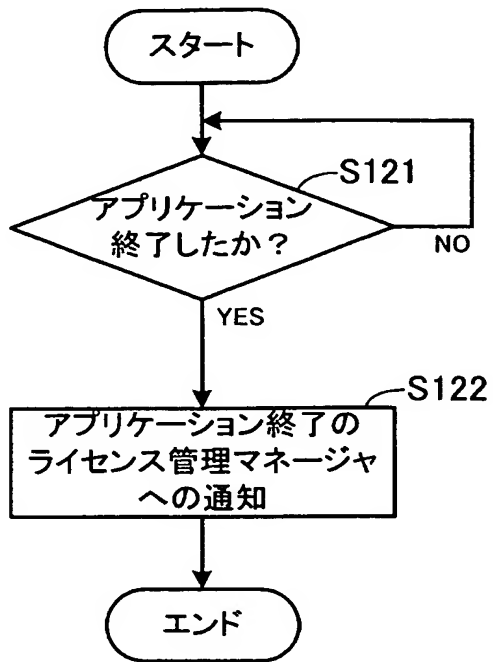
【図 31】



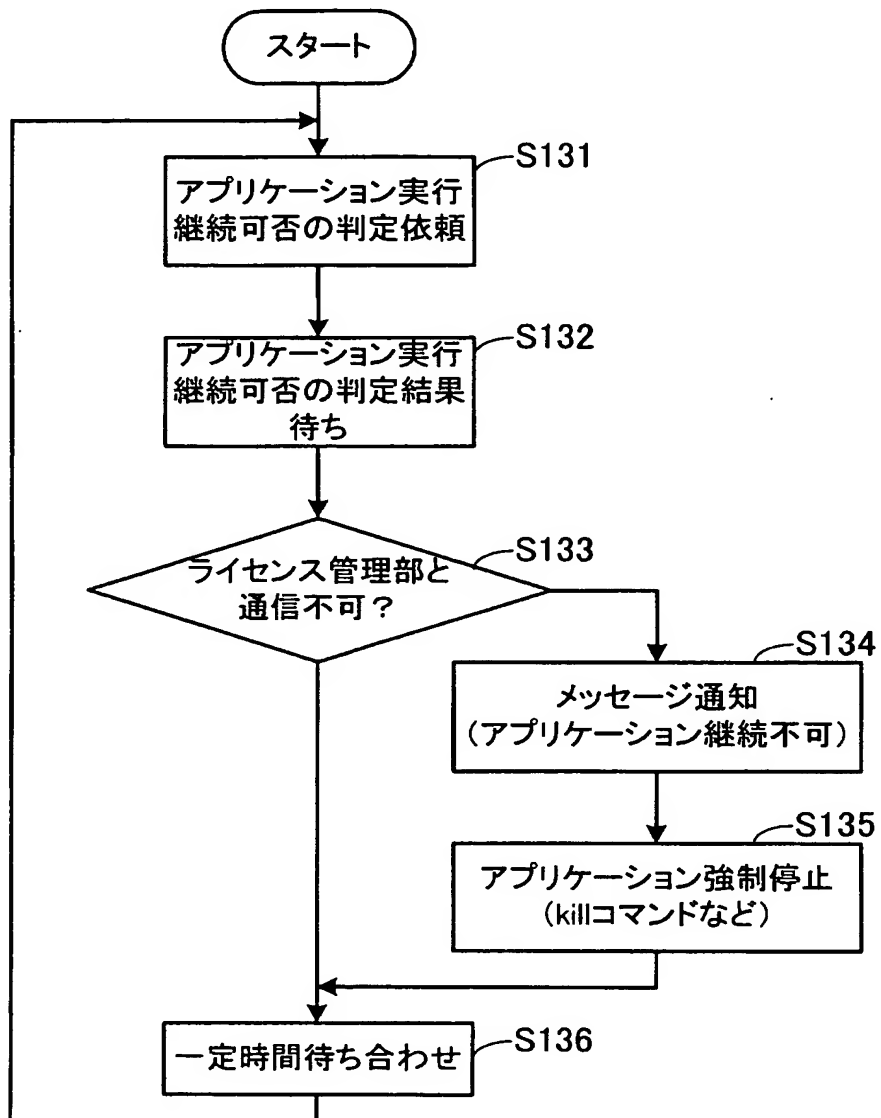
【図 32】



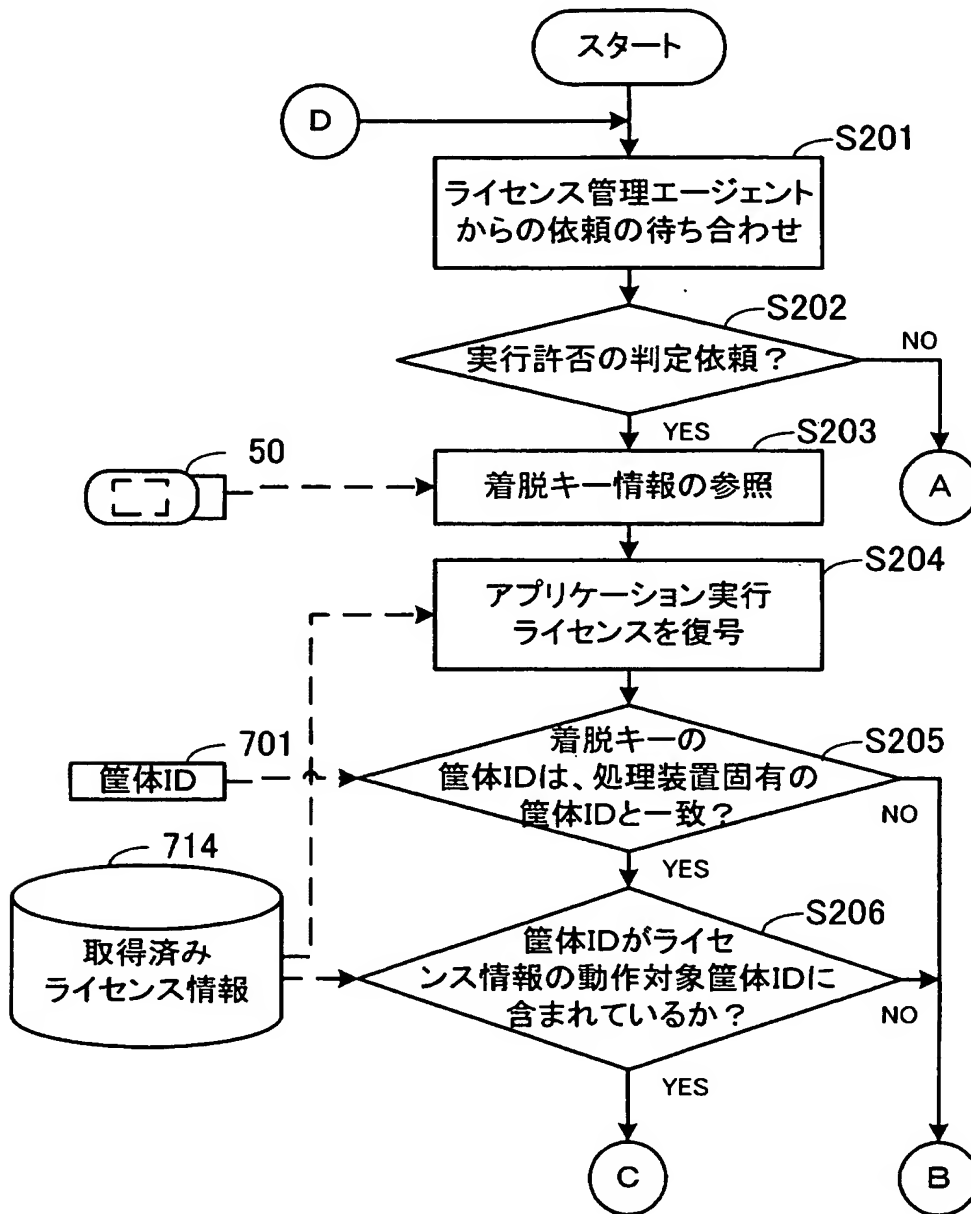
【図 33】



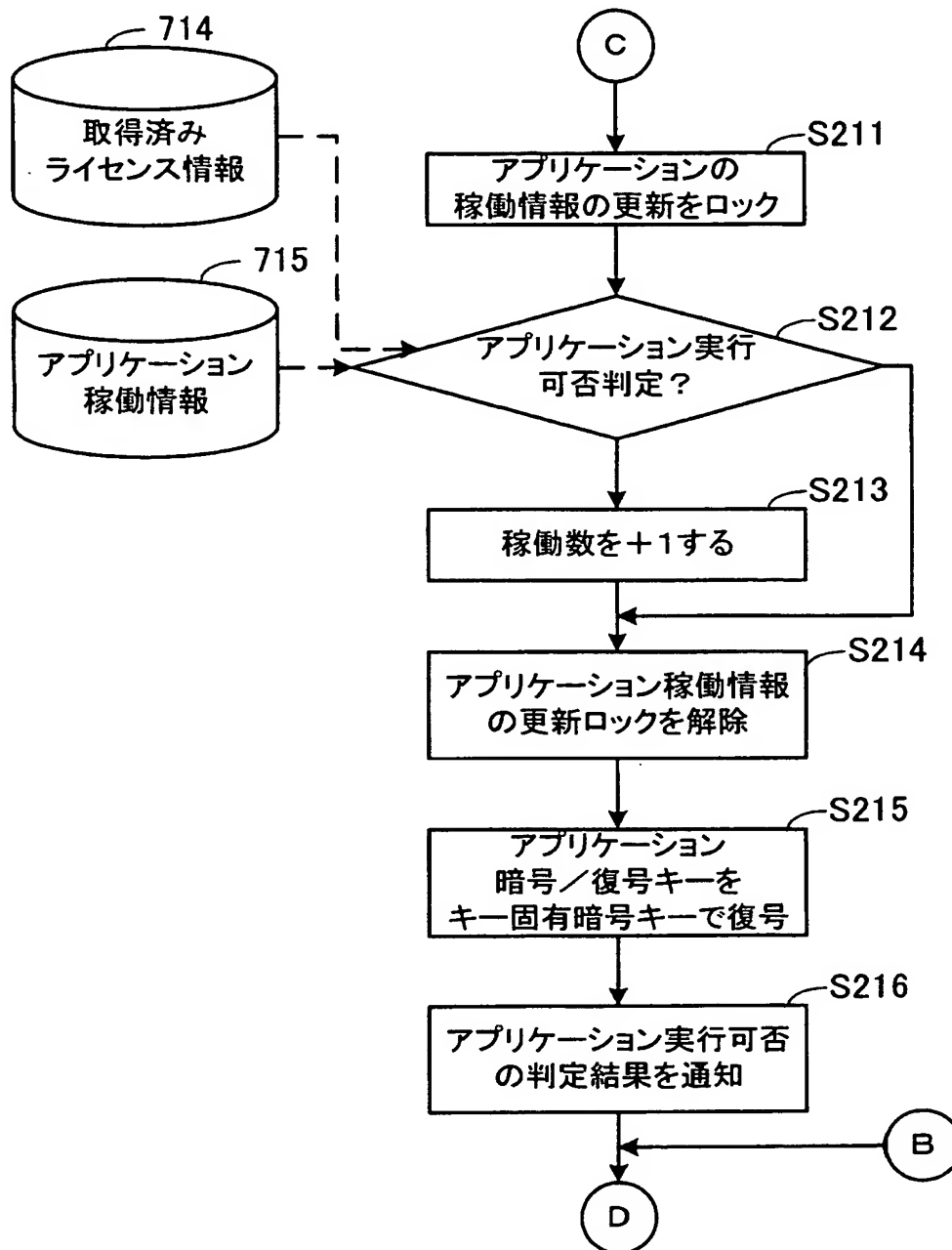
【図 34】



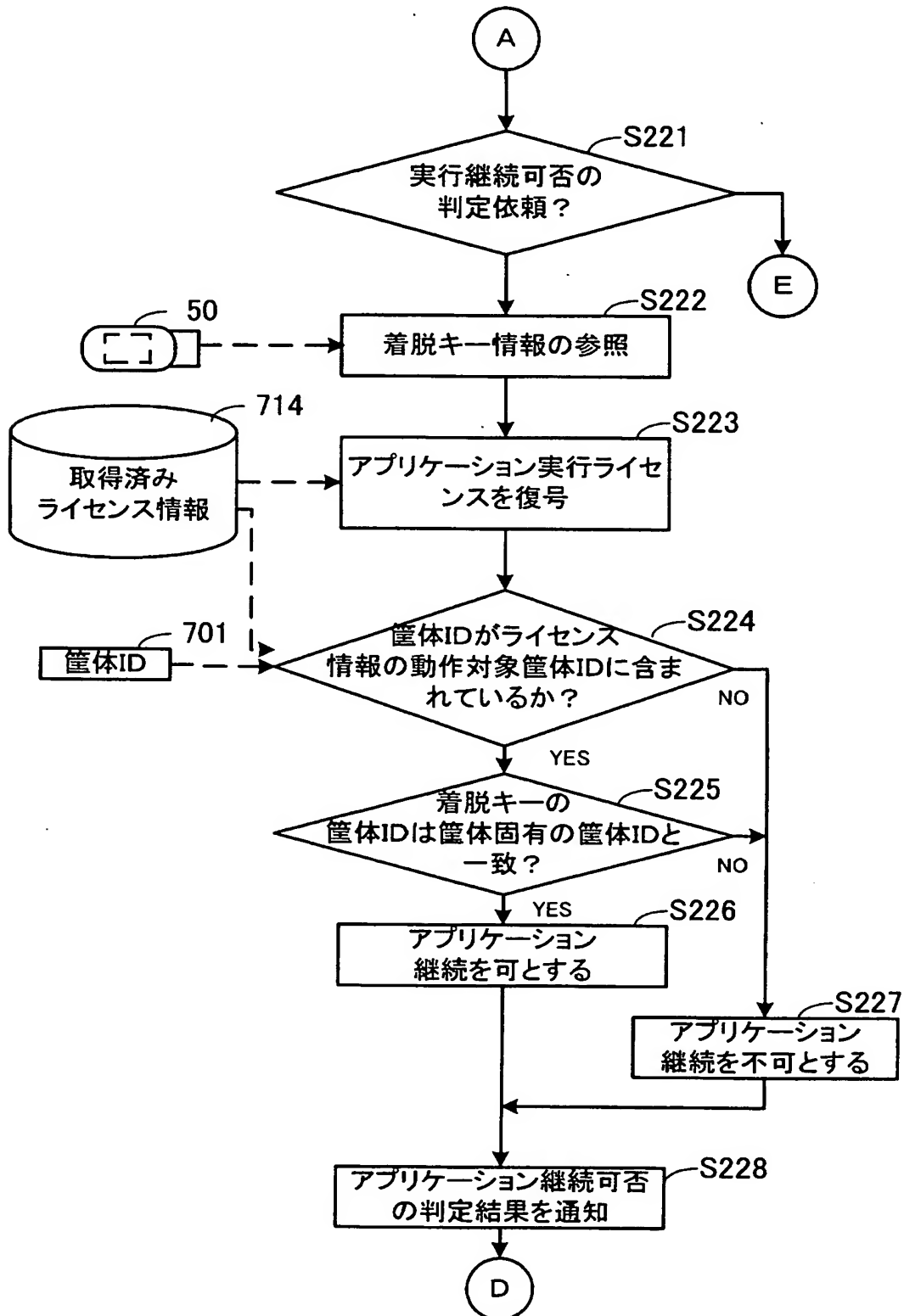
【図 35】



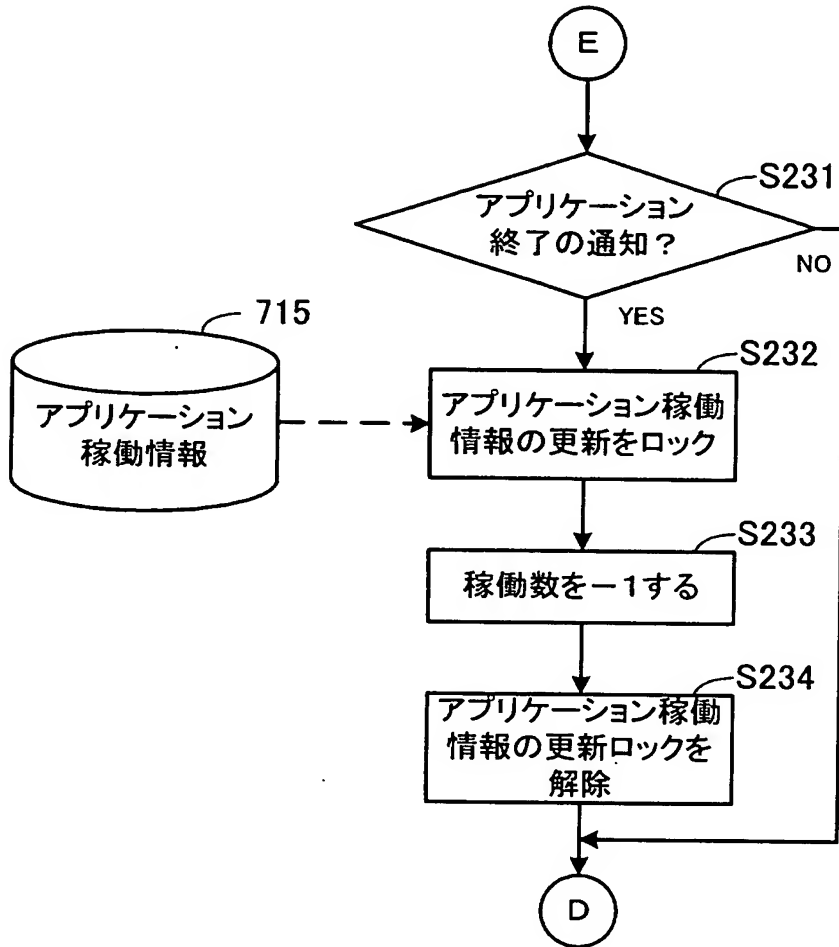
【図 36】



【図 37】



【図 38】



---

【書類名】 要約書

【要約】

【課題】 マシン毎のライセンス供与に関する強固な不正防止機能を実現する。

【解決手段】 ソフトウェア暗号キー生成手段 1 は、ソフトウェア 6 a の暗号化のための暗号キー生成要求に応じて、ソフトウェア暗号キー 5 a と、ソフトウェア暗号キー 5 a で暗号化されたソフトウェア 6 b を復号するためのソフトウェア復号キー 5 b とを生成する。ライセンス発行手段 2 は、ソフトウェア 6 a の動作許可対象である処理装置 4 内の記録媒体 4 a に固定的に記録された装置識別情報 4 b を含むライセンス発行要求に応じて、装置識別情報 4 b でソフトウェア復号キー 5 b を暗号化し、暗号化されたソフトウェア復号キーを含むソフトウェアライセンス 5 c を出力する。これにより、装置識別情報 4 b が固定的に記録された処理装置 4 でのみ暗号化されたソフトウェアを復号することが可能となる。

【選択図】 図 1



特願 2002-274845

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1990年 8月24日  
[変更理由] 新規登録  
住 所 神奈川県川崎市中原区上小田中1015番地  
氏 名 富士通株式会社
2. 変更年月日 1996年 3月26日  
[変更理由] 住所変更  
住 所 神奈川県川崎市中原区上小田中4丁目1番1号  
氏 名 富士通株式会社